

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»**

**Інститут телекомунікаційних систем
Кафедра Інформаційно-телекомунікаційних мереж**

До захисту допущено:

Завідувач кафедри

_____ Лариса ГЛОБА

«__» _____ 2020 р.

**Дипломна робота
на здобуття ступеня бакалавра
за освітньо-професійною програмою «Інформаційно-комунікаційні
технології»
спеціальності 172 «Телекомунікації та радіотехніка»
на тему: «Аналіз рішень для систем керування потоками Інтернету
речей»**

Виконала:

студентка IV курсу, групи ТІ-62

Брей Анастасія Миколаївна _____

Керівник:

Професор кафедри ІТМ ІТС, д.т.н., с.н.с.

Скулиш Марія Анатоліївна _____

Рецензент:

Доцент кафедри ТК ІТС, к.т.н.

Міночкін Дмитро Анатолійович _____

Засвідчую, що у цій дипломній роботі
немає запозичень з праць інших
авторів без відповідних посилань.

Студентка _____

Київ – 2020 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
Кафедра Інформаційно-телекомунікаційних мереж

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Інформаційно-комунікаційні технології»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Лариса ГЛОБА

«__» _____ 2020 р.

ЗАВДАННЯ
на дипломну роботу студенту
Брей Анастасія Миколаївна

1. Тема роботи «Аналіз рішень для систем керування потоками Інтернет речей», керівник роботи професор кафедри інформаційно-телекомунікаційних мереж ІТС Скулиш Марія Анатоліївна, д.т.н., с.н.с., затверджені наказом по університету від «30» березня 2020 р. № 924-с.

2. Термін подання студентом роботи 8 червня 2020 р.

3. Вихідні дані до роботи: праці іноземних вчених, матеріали мережі інтернет, власні спостереження та знання, матеріали з підручників.

4. Зміст роботи:

- 1) Розглянути роль та місце IoT в інформаційних системах;
- 2) Проаналізувати основні протоколи і формати обміну даними між компонентами системи управління потоками;
- 3) Провести аналіз існуючих програмно-апаратних рішень для систем управління потоками;

4) Проаналізувати проблеми управління потоками даних в IoT та вирішення цих проблем.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)

6. Дата видачі завдання 05.11.2019 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Провести аналіз історії IoT	10.01.2020 р. 27.01.2020 р.	виконано
2	Визначити перспективи використання IoT	28.01.2020 р. 17.02.2020 р.	виконано
3	Проаналізувати архітектуру IoT	18.02.2020 р. 02.03.2020 р.	виконано
4	Провести аналіз існуючих систем управління потоками	03.03.2020 р. 20.03.2020 р.	виконано
5	Визначити протоколи і формати обміну даними між компонентами системи управління потоками	21.03.2020 р. 15.04.2020 р.	виконано
6	Вивчити та проаналізувати програмно-апаратні рішення для системи управління потоками	16.04.2020 р. 28.04.2020 р.	виконано
7	Розглянути сучасні проблеми управління потоками даних в IoT	29.04.2020 р. 15.05.2020 р.	виконано
8	Проаналізувати можливі рішення проблем управління даними	16.05.2020 р. 31.05.2020 р.	виконано

Студент

Анастасія БРЕЙ

Керівник

Марія СКУЛИШ

РЕФЕРАТ

Робота містить 90 сторінок, 8 рисунків та 6 таблиць. Було використано 21 джерело.

Мета роботи: підвищення ефективності обробки інформаційних потоків в системах IoT за рахунок вибору оптимального способу керування потоками відповідно до специфічних вимог та особливостей системи.

В даній роботі розглядається система управління потоками даних IoT. Було розглянуто основні протоколи і формати обміну даними між компонентами системи управління потоками.

Проаналізовано існуючі програмно-апаратні рішення для систем управління потоками та проаналізовано керування даними в цих системах.

Визначено загальні характеристики даних в IoT та розглянуто еталонну модель управління даними IoT, яка складається з трьох шарів. Проведено аналіз типових проблеми, що зустрічаються в кожному рівні еталонної моделі управління даними IoT та їх можливих рішень.

Ключові слова: IoT, потоки даних, система управління, протокол, стандарт.

ABSTRACT

The work contains 90 pages, 8 drawings and 6 table. Twenty-one sources were used.

Goal: to improve the efficiency of information flow processing in IoT systems by choosing the best way to manage the flow in accordance with specific requirements and features of the system.

In this paper IoT data flow management system is considered. The main protocols and formats of data exchange between the components of the flow control system were considered.

Existing hardware and software solutions for flow control systems were analyzed and data management in these systems was analyzed.

General characteristics of data in IoT are determined and a reference model of IoT data management, which consists of three levels, is considered. Typical problems encountered in each level of the IoT data management reference model and their possible solutions are analyzed.

Keywords: IoT, data flows, control system, protocol, standard.

ЗМІСТ

ВСТУП	11
РОЗДІЛ 1.....	13
РОЛЬ І МІСЦЕ ІНТЕРНЕТУ РЕЧЕЙ В ІНФОРМАЦІЙНИХ СИСТЕМАХ..	13
1.1. Історія IoT.....	13
1.2. Застосування та перспективи використання IoT.....	14
1.3. Архітектура IoT	18
1.3.1. Рівень датчиків та сенсорних мереж.	19
1.3.2. Рівень шлюзів та мереж.....	20
1.3.3. Сервісний рівень.....	21
1.3.4. Рівень додатків	21
РОЗДІЛ 2.....	23
АНАЛІЗ СИСТЕМИ УПРАВЛІННЯ ПОТОКАМИ ІОТ	23
2.1. Протоколи та формати обміну даними між компонентами системи управління потоками	25
2.1.1. Стандарт IEEE Std 802.15.4.....	25
2.1.2. Стандарт ZigBee	28
2.1.3. Стандарт 6LoWPAN.....	31
2.1.4. Стандарти Wireless Hart і ISA100.11a	34
2.1.5. Стандарт Z-Wave.....	38
2.1.6. Стандарт Bluetooth Low Energy	40
2.1.7. Сімейство стандартів IEEE 802.11	43
2.1.8. Стандарт DECT ULE.....	46

2.1.9. Протокол MQTT	48
2.2. Керування даними в програмно-апаратних рішеннях для систем управління потоками	50
2.2.1. Розумна планета	50
2.2.2. Розумне місто.....	52
2.2.3. Розумний будинок.....	53
2.2.4. Розумна енергія	57
2.2.5. Розумний транспорт.....	59
2.2.6. Розумне виробництво.....	61
2.2.7. Розумна медицина	64
2.2.8. Розумне життя	65
Висновки:	66
РОЗДІЛ 3.....	67
АНАЛІЗ ПРОБЛЕМ УПРАВЛІННЯ ПОТОКАМИ ДАНИХ В ІОТ	67
3.1 Загальні характеристики даних IoT	67
3.2 Еталонна модель управління даними IoT	68
3.3 Проблеми управління даними IoT та підходи до їх вирішення.....	69
ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ	86
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	88

ПЕРЕЛІК СКОРОЧЕНЬ

IoT	Internet of Things
TCP/IP	Transmission Control Protocol/Internet Protocol
RFID	Radio Frequency Identification
NGN	Next Generation Network
LAN	Local Area Network
PAN	Personal Area Network
WAN	Wide Area Network
MAN	Metropolitan Area Network
GSM	Global System for Mobile
GPRS	General Packet Radio Service
LTE	Long-Term Evolution
WSN	Wireless sensor network
M2M	Machine-to-Machine
OSS	Operation Support System
BSS	Business Support System
BPM	Business Process Management
BRM	Business Rule Management
QoS	Quality of Service
QoE	Quality of Experience
NFC	Near-field communication
WiMAX	Worldwide Interoperability for Microwave Access
PLC	Power Line Communication
WPAN	Wireless Personal Area Network
TAN	Tiny Area Network
ISM	Industrial Scientific Medical
DSSS	Direct Sequence Spread Spectrum

QPSK	Quadrature Phase Shift Keying
UWB	Ultra WideBand
CSS	Chirp Spread Spectrum
GFSK	Gaussian Frequency-Shift Keying
BPSK	Binary Phase-Shift Keying
RFD	Reduced Function Device
P2P	peer-to-peer, point-to-point
RF4CE	Radio Frequency for Consumer Electronics
6LoWPAN	IPv6 Low-Power Wireless Personal Area Network
ARP	Address Resolution Protocol
TDMA	Time-division multiple access
ISA	International Society of Automation
FHSS	Frequency Hopping Spread Spectrum
CDMA	Code-Division Multiple Access
UAP	Ukrainian Academy of Printing
OSI	Open Systems Interconnection
IETF	Internet Engineering Task Force
GFSK	Gaussian frequency shift keying
BLE	Bluetooth Low Energy
L2CAP	Logical Link Control and Adaptation Protocol
GATT	Generic Attribute Profile
SMP	Security Manager Protocol
GAP	Generic Access Profile
HCI	Host Controller Interface
PCF	Point Coordination Function
DCF	Distributed Coordination Function
CCK	Complementary Code Keying
OFDM	Orthogonal frequency-division multiplexing
MU-MIMO	Multi-User Multiple-Input / Multiple-Output

DECT ULE	Digital European Cordless Telecommunications Ultra Low Energy
MQTT	Message Queuing Telemetry Transport
HTTP	The Hypertext Transfer Protocol
ESP	Extensible Sensor stream Processing
PML	Physical Markup Language
SOA	Service-oriented architecture

ВСТУП

Актуальність теми даної роботи обумовлена тим, що технологія IoT дозволить з легкістю контролювати всі аспекти нашого життя. Нинішня технічна революція, та швидкий розвиток мобільних технологій можна вважати першою фазою Інтернету речей. Число фізичних об'єктів, підключених до інтернету зростає з безпрецедентною швидкістю, що реалізує ідею Інтернету речей. Технологія розумних речей здатна підвищити продуктивність праці в першу чергу в виробничому сегменті, логістичному бізнесі, транспортних і енергетичних компаніях. Складність впровадження полягає в тому, що жоден виробник не має в своєму складі закінченого рішення, що включає всі компоненти. Необхідно використання великої кількості систем від різних виробників і від їх правильного підбору та інтеграції залежить те, наскільки точно реалізоване рішення буде відповідати завданням і вимогам конкурентного середовища.

Мета роботи: підвищення ефективності обробки інформаційних потоків в системах IoT за рахунок вибору оптимального способу керування потоками відповідно до специфічних вимог та особливостей системи.

Виходячи з цього, **основні завдання дослідження** полягають у наступному:

- 1) Дослідити потенціальні можливості та проблеми IoT в інформаційних системах;
- 2) Проаналізувати основні протоколи і формати обміну даними між компонентами системи управління потоками;
- 3) Провести аналіз існуючих програмно-апаратних рішень для систем управління потоками та розглянути керування даними в цих системах.
- 4) Проаналізувати проблеми управління потоками даних в IoT та розглянути підходи до вирішення цих проблем.

Об’єкт дослідження: мережа Інтернет речей.

Предмет дослідження: системи управління потоками IoT .

Теоретичний результат дослідження:

Проведено аналіз існуючих програмно-апаратних рішень для систем управління потоками та розглянуто керування даними в цих системах.

Досліджено основні проблеми управління потоками даних в IoT.

Практичний результат дослідження:

Запропоновані підходи, щодо проблем управління потоками даних в IoT можуть бути використані для підвищення ефективності обробки інформаційних потоків даних в системах Інтернету речей.

РОЗДІЛ 1.

РОЛЬ І МІСЦЕ ІНТЕРНЕТУ РЕЧЕЙ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

1.1. Історія IoT

Інтернет речей (The Internet of Things, IoT) - це новий етап розвитку Інтернету, який значно розширює можливості збору, аналізу і розподілу даних, які людина може перетворити в інформацію і в знання. Інтернет речей (IoT) пов'язує об'єкти з Інтернетом, що дозволяє аналізувати та отримувати дані, які раніше були недоступні. Концепція IoT дозволяє не тільки об'єднувати предмети матеріального світу за допомогою інтернету для обміну інформацією між ними, а й розвивати можливості по накопиченню, структуруванню та аналізу різної інформації. Під Інтернетом речей передбачають не тільки безліч різних приладів і датчиків, об'єднаних між собою дротовими та бездротовими каналами зв'язку і підключених до мережі Інтернет, але й більш тісну інтеграцію реального та віртуального світів, в якому спілкування проводиться між людьми та пристроями.

У тих випадках, коли IoT розглядається одночасно як технічний та культурний феномен, його історію ведуть з 9 жовтня 1832 р., коли видатний російський дипломат і вчений Павло Львович Шилінг продемонстрував у своєму будинку на Марсовому полі в Санкт-Петербурзі першу чинну модель електромагнітного телеграфу. З цього моменту почалася передача даних з використанням електричної енергії.

У 1926 р. Нікола Тесла в інтерв'ю для журналу «Collier's» сказав: "Коли бездротові технології досягнуть справжнього розвитку, вся Земля перетвориться в єдиний величезний мозок, всі речі стануть частиною єдиного цілого і доступ до цього мозку людина матиме за допомогою приладу, схожого на сучасний телефон, та кожен зможе носити його в кишені". Важко повірити, що ці слова були вимовлені 94 роки тому.

У 1990 р. випускник МІТ, один з батьків протоколу TCP/IP, Джон Ромки винайшов першу у світі інтернет-річ. Він зумів приєднати до мережі свій тостер. Інженер зміг, приєднавши кухонного помічника до всесвітньої павутини, ввімкнути та вимкнути його віддалено. Він зробив це просто так, заради забави, не підозрюючи, що його експеримент стане спусковим механізмом, який викличе у багатьох "ефект лавини" та почне формувати нову реальність. Надалі концепція поступово розвивалася, ускладнювалася, знаходила теоретичну базу та практичний сенс.

У 1999 р. Кевіном Ештоном був запропонований термін "Інтернет речей" (Internet of Things). У цьому ж році був створений Центр автоматичної ідентифікації (AutoID Center), що займався радіочастотною ідентифікацією (RFID) і сенсорними технологіями, завдяки якому ця концепція і набула дуже широкого поширення.

У 2008-2009 рр. відбувся перехід від «Інтернету людей» до «Інтернету речей», тобто кількість підключених до мережі предметів перевищила кількість людей[1].

На сьогодні день існує можливість ідентифікувати обладнання, предмети побуту та віртуальні об'єкти (наприклад, цифрові фотографії) таким же чином, як і окремих користувачів в Інтернеті людей. Таким чином, речі можуть бути інтегровані в широку мережу взаємозв'язків, в якій вони можуть взаємодіяти один з одним або з людьми. Фактично, речі у світі IoT тепер знаходяться на одному рівні з людьми.

1.2. Застосування та перспективи використання IoT

IoT має великий потенціал для розвитку майже у всіх сферах, які в основному завдяки Інтернету речей можуть бути контекстно-залежними (наприклад, можуть збирати інформацію про природні параметри, медичні параметри або звички користувача), а також надавати індивідуальні послуги.

Незалежно від області застосування, метою цих додатків є підвищення якості повсякденного життя людей та великий вплив на економіку та суспільство. Застосування IoT можна поділити на три області: промислову, область «розумного міста» та область охорони здоров'я. Кожна частина не є окремою, а частково перекривається, оскільки деякі програми спільні. Наприклад, відстеження продуктів, як правило, у галузі промисловості та у галузі охорони здоров'я, можна використовувати для спостереження за товарами або продуктами харчування, але також відстеження продуктів можна використовувати для контролю розподілу лікарських засобів[2].

Таблиця 1.1

Основні сфери застосування Інтернету речей

Область застосування	Сегментація	Приклади
Розумне місто	Розумний будинок	Домашня мережа
		Управління мультимедіа, управління електроживленням
	Громадська безпека та екологічний моніторинг	Моніторинг навколишнього середовища
		Інтелектуальні мобільні пристрої
Охорона здоров'я	Діагностика і лікування захворювань	Моніторинг життєво важливих ознак
	Незалежне життя	Допомога інвалідам
		Екстрений порятунок

Продовження таблиці 1.1

Промислова	Логістика та життєвий цикл продукції	Управління запасами, вантажні перевезення
		Консервація їжі
	Сільське господарство та тваринництво	Сільськогосподарське виробництво та розведення
		Контроль за інфекційними захворюваннями тварин
	Промислові процеси	Діагностика транспортних засобів в режимі реального часу
		Управління багажем

У таблиці 1.1 показано розподіл вищезазначених областей застосування IoT. Варто зазначити, що не всі IoT програми мають однаковий рівень розвитку. Деякі з цих додатків вже є частиною нашого повсякденного життя, але більшість з них ще перебувають на стадії експерименту. Зокрема, існує багато різних додатків на стадії розробки.

Закордонна практика демонструє успішний досвід впровадження Інтернету речей як на державному рівні, так і на приватному. Прикладами можуть бути країни ЄС, Південна Корея, Китай та Індія.

Використання в закордонній практиці технологій «Розумного міста» дозволяє підвищувати ефективність управління енергоспоживанням і транспортними потоками. Більш того, в таких країнах, як Великобританія і США, вже діють масштабні програми з впровадження «розумних лічильників», які віддалено контролюють енергоспоживання в домогосподарствах[3].

На сьогоднішній день можна впевнено говорити про економічний ефект від застосування технологій Інтернету речей в галузі сільського

господарства. За прогнозами ООН до 2050 р. для задоволення потреби населення Землі в їжі необхідно буде збільшити виробництво продуктів харчування на 70% в порівнянні з поточним. Для галузі сільського господарства це може означати постійно зростаючий попит на вироблену ними продукцію, а також необхідність нових правил для виробництва в цілому. «Розумне сільське господарство» має мету запровадити максимальну автоматизацію сільськогосподарської діяльності. При цьому має збільшуватися не тільки врожайність, але і якість продукції. Досягти цієї мети планується за рахунок впровадження повсюдного контролю у витрачання сировини, а також зберігання самої продукції. Наприклад, у вирощуванні овочів та фруктів використання різних датчиків, пристроїв, а також програмного забезпечення для віддаленого управління допоможе зменшити використання агрохімікатів, добрив, а також води аж до 15-20%. Застосування технологій моніторингу і контролю на фермах, реалізованих у вигляді автоматизації системи годування, доїння та моніторингу здоров'я худоби, в кінцевому рахунку дозволить підвищити надої на 30-40%.

Технології IoT активно впроваджуються в охорону здоров'я. На сьогодні, технології корисні тим, що є можливість відстежувати стан здоров'я пацієнтів віддалено. У найближчому майбутньому пацієнти зможуть не відвідувати лікаря для вимірювання кров'яного тиску, так як датчики самі передадуть до лікарні всі дані. Якщо людина сильно захворіє, то лікар дізнається про це відразу.

Статистика підключених пристроїв безперервно зростає, покращуючи мікроклімат в клініках. Ця тенденція збережеться, тому що великі компанії постійно шукають нові ринки збуту своєї продукції[4].

Аналізуючи можливі прогнози щодо розвитку Інтернету речей можна припустити досить великий стрибок витрат на розвиток Інтернету речей. На даний час найбільшу зацікавленість IoT придбав у сферах програм, дискретних виробництв, а також у сфері транспорту і логістики. Причому

показники цих витрат можуть збільшитися більше ніж у два рази. Цей показник є позитивним, так як він відображає зацікавленість у сфері IoT і бажання в його активному інвестуванні і розвитку. Таким чином, з кожним роком перспектива впровадження технологій IoT в усі сфери нашого життя постійно збільшується.

Однак на даний момент активному розвитку ринку IoT заважають декілька речей. Найбільш актуальною проблемою зараз є відсутність будь-яких стандартів. Якщо брати до уваги загальне поширення технології IoT, то вкрай необхідно забезпечити унікальність ідентифікаторів кожного з об'єктів, що знаходиться в цій мережі. Відсутність певних стандартів досить сильно стримує індустрію IoT від розвитку і повсюдної інтеграції її рішень.

Наступною проблемою в реалізації повної автономності систем IoT є нездатність датчиків працювати незалежно від змінних або вимагаючих заряду пристроїв живлення. В цьому плані підключеним пристроям необхідно навчитися виробляти енергію з навколишнього середовища.

У разі широкої популяризації технології IoT особливу важливість також набувають питання безпеки самої системи. Легко припустити, які можливі наслідки може спричинити за собою недостатня забезпеченість системи, відсутність в ній необхідних протоколів безпеки та шифрування даних[5].

1.3. Архітектура IoT

IoT взагалом відноситься до мереж наступного покоління, тому його архітектура багато в чому схожа з архітектурою NGN. Інтернет речей складається з набору різних телекомунікаційних технологій, що забезпечують функціонування IoT. За допомогою його архітектури, маємо змогу розглянути, як ці технології пов'язані одна з одною. Архітектура IoT

складається з чотирьох функціональних рівнів (рисунок 1.1), описаних нижче[6].

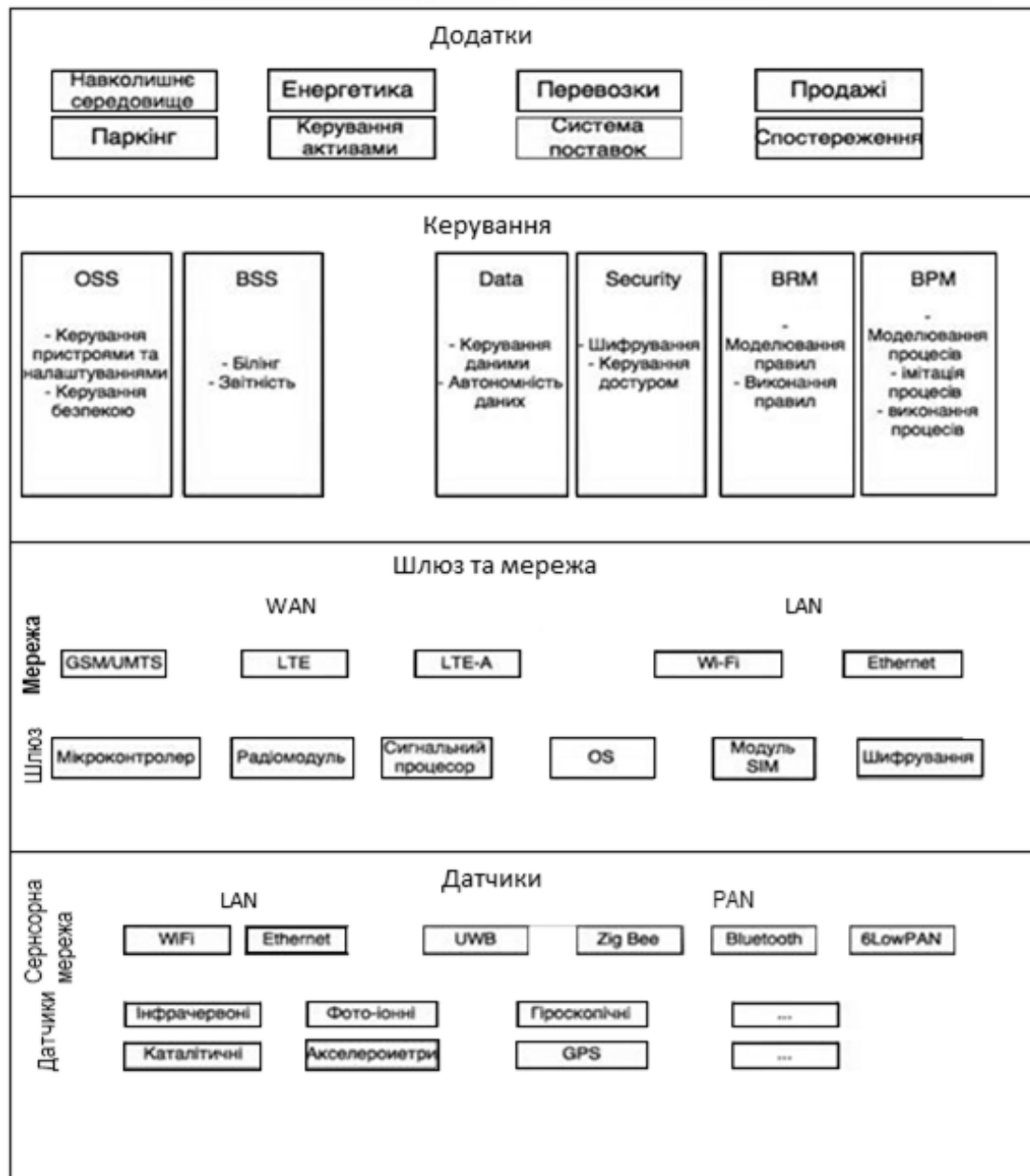


Рис. 1.1 Архітектура IoT

1.3.1. Рівень датчиків та сенсорних мереж.

До першого рівня архітектури відносять «розумні» (smart) об'єкти, інтегровані з датчиками (сенсорами). За допомогою датчиків можна реалізувати поєднання віртуального (цифрового) та фізичного світів,

надаючи можливість збору та обробки інформації в реальному часі. Мініатюризація, що призвела до зменшення фізичних розмірів апаратних сенсорів, дозволила інтегрувати їх безпосередньо в об'єкти фізичного світу. Є різні типи сенсорів для конкретних цілей, наприклад, для вимірювання тиску, температури, струму, та інші. Сенсори мають можливість нотувати результати вимірювань, маючи невелику пам'ять. Датчики мають можливість вимірювати фізичні параметри контрольованого явища/ об'єкта і перетворювати їх в сигнал, який може бути прийнятий відповідним пристроєм. Класифікувати сенсори можна за їх призначенням, наприклад, сенсори для техніки, сенсори для тіла, сенсори для транспортних засобів і т. п.

Велика частина датчиків вимагає поєднання з агрегатором сенсорів (шлюзом), які можуть бути виконані з використанням локальної обчислювальної мережі (LAN, Local Area Network), таких як Wi-Fi та Ethernet або персональної мережі (PAN, Personal Area Network). Для сенсорів, що не вимагають підключення до агрегатора, зв'язок з додатками/серверами може надаватися з використанням глобальних бездротових мереж WAN, таких як GSM, GPRS і LTE.

Сенсори з малим енергоспоживанням та повільною швидкістю передачі даних, утворюють бездротові сенсорні мережі (WSN, Wireless Sensor Network).

1.3.2. Рівень шлюзів та мереж

Чимала кількість даних, що створюється сенсорами на першому рівні IoT, вимагає надійної та високопродуктивної проводової або бездротової мережевої інфраструктури в якості транспортного середовища. Мережі зв'язку, що використовують різні протоколи, можна застосувати для підтримки міжмашинних комунікацій M2M та їх додатків. Для можливості

виконання великої кількості різних послуг і додатків в IoT необхідно забезпечити спільну роботу багатьох різних технологій і протоколів доступу в гетерогенній конфігурації. Такі мережі повинні забезпечувати потрібні значення якості передачі інформації, і більш за все по затримці, пропускній спроможності та безпеці. Даний рівень складається з конвергентної мережевої інфраструктури, яку можна створити за допомогою інтеграції гетерогенних мереж в єдину мережеву платформу. Мережевий рівень надає змогу декільком користувачам через відповідні шлюзи використовувати ресурси в одній мережі без шкоди для конфіденційності, безпеки та продуктивності.

1.3.3. Сервісний рівень

Сервісний рівень складається з набору інформаційних послуг, за допомогою яких можна автоматизувати технологічні та бізнес операції в IoT: підтримки операційної та бізнес діяльності (OSS / BSS, Operation Support System / Business Support System), різної аналітичної обробки інформації (статистичної, інтелектуального аналізу даних і текстів, прогностичної аналітики та ін.), зберігання даних, управління бізнес-процесами (BPM, Business Process Management), управління бізнес-правилами (BRM, Business Rule Management) та ін.

1.3.4. Рівень додатків

На четвертому рівні архітектури є багато різних типів додатків для відповідних промислових секторів і інших сфер діяльності (освіта, транспорт, торгівля, медицина та ін.). Додатки можуть бути «вертикальними», коли вони є специфічними для конкретної галузі промисловості, а також «горизонтальними», (наприклад, управління

автопарком, відстеження активів та ін.), Які можуть використовуватися в різних секторах економіки[7].

Висновки:

Інтернет речей може стати наступним кроком вперед у сфері інформаційно-комунікаційних технологій. Масштабне розгортання вбудованих додатків збільшує можливість плавного злиття реального та віртуального світів, відкриття нових напрямків досліджень та бізнесу. З кожним днем перспектива впровадження технологій IoT в усі сфери нашого життя стрімко збільшується.

У цьому розділі було вирішено такі завдання:

1. Коротко розглянуто історію виникнення Інтернету речей, представлені найбільш актуальні сфери застосування та перспективи використання IoT.
2. Приведені загальні проблеми розвитку ринку Інтернет речей.
3. Проведено огляд існуючої архітектури IoT.

РОЗДІЛ 2.

АНАЛІЗ СИСТЕМИ УПРАВЛІННЯ ПОТОКАМИ ІОТ

Одним з головних питань організації Інтернету речей є реалізація взаємодії між:

- інтернет-речами,
- користувачами та інтернет-речами,
- віддаленим сервером і інтернет-речами.

ІоТ використовує велику кількість варіантів мереж зв'язку для передачі даних, починаючи від мережі на тілі людини BAN (Body Area Network), яка працює на відстані в кілька десятків сантиметрів, аж до всесвітньої мережі інтернет. Комунікації малої дальності використовують такі технології, як RFID, NFC, Bluetooth, Wi-Fi та ін. Комунікації великого радіусу дії реалізуються на базі різних стільникових мереж (2G/3G/4G), мереж бездротового широкосмугового доступу WiMAX, мереж позиціонування GPS та ін.

Територію охоплення телекомунікаційних мереж, які використовуються в Інтернеті речей, можна розділити на 4 основні типи:

1. WAN
2. MAN
3. LAN
4. PAN

1. Персональна мережа PAN (Personal Area Network) - ця мережа побудована «навколо» людини. Дані всієї мережі об'єднують чимало персональних пристроїв користувачів (ноутбуки, смартфони, кишенькові персональні комп'ютери, гарнітури та ін.). Стосовно до ІоТ така мережа будується «навколо» пристроїв («речей»).

2. Локальна мережа LAN (Local Area Network) - мережа, яка у більшості випадків покриває відносно невелику територію чи невелику

групу будівель (будинок, офіс). До таких мереж можна віднести й мережу контролерів CAN (Controller Area Network) – промислову мережу, яка перш за все, орієнтується на поєднання в єдину мережу різних виконавчих датчиків та присторів в рамках окремого підприємства.

3. Міська мережа MAN (Metropolitan Area Network) - об'єднує окремих користувачів і локальні мережі в межах міста, являє собою мережу за розмірами більшу, ніж LAN, але меншу, ніж WAN.

4. Глобальна мережа WAN (Wide Area Network) - пов'язує користувачів і мережі, зосереджених на відстані сотень та тисяч кілометрів[8].

Інтернет речей практично не висуває особливих вимог до технологій LAN, MAN і WAN, крім того вони досить добре освітлені в технічній літературі. Тому в цьому розділі розглянуто лише стандарти та протоколи мереж малого і середнього радіусу дії, які широко використовуються в IoT.

Всі технології передачі даних в Інтернеті речей в залежності від використовуваного середовища передачі можна розділити на два великі класи: провідні та бездротові.

Провідні технології передачі даних в IoT можуть використовувати металевий (мідний) кабель зв'язку, електропроводку (технологія PLC - Power Line Communication) або волоконно-оптичний кабель. Однак, зважаючи на складнощі фізичної реалізації ліній зв'язку провідні технології для комунікацій інтернет-речей застосовуються в меншій мірі, ніж бездротові.

Бездротові мережі малого радіусу дії, які використовуються в IoT, можна розділити на три види:

1) Бездротові персональні мережі WPAN (Wireless Personal Area Network). Застосовуються для зв'язку різних пристроїв, включаючи комп'ютерну, побутову та оргтехніку, засоби зв'язку і т.д. Фізичний і канальний рівні регламентуються стандартом IEEE 802.15.4. Радіус дії WPAN становить від кількох метрів до кількох десятків сантиметрів. Такі мережі використовуються як для об'єднання окремих пристроїв між собою,

так і для зв'язку їх з мережами більш високого рівня, наприклад, глобальною мережею інтернет. WPAN може бути розгорнута з використанням різних мережевих технологій, наприклад, Bluetooth, ZigBee, 6LoWPAN і інших, розглянутих далі в цьому розділі.

2) Бездротові сенсорні мережі WSN (Wireless Sensor Network). Розподілені, самоорганізаційні мережі з безліччю датчиків (сенсорів) виконавчих пристроїв, об'єднаних між собою за допомогою радіоканалу. Область покриття подібних мереж може становити від декількох метрів до декількох кілометрів за рахунок здатності ретрансляції повідомлень від одного елемента до іншого.

3) Малі локальні мережі TAN (Tiny Area Network). Обчислювальні мережі, що розгортаються в межах невеликого офісу або окремого житла. Їх часто називають домашніми мережами, так як вони об'єднують комп'ютери, побутову електроніку і прилади сигналізації, що належать одній родині. Найбільш часто такі мережі будуються на базі технології Wi-Fi[9].

2.1. Протоколи та формати обміну даними між компонентами системи управління потоками

Для взаємодії величезної кількості різноманітних пристроїв в IoT потрібні стандартизовані інтерфейси, формати даних і комунікаційні протоколи.

2.1.1. Стандарт IEEE Std 802.15.4

Стандарт IEEE Std 802.15.4 призначений для реалізації бездротових персональних мереж WPAN великої місткості з низьким енергоспоживанням і низькою швидкістю передачі даних. Він реалізує тільки два нижніх рівні стека протоколів: фізичний рівень (PHY) і рівень доступу до середовища

(MAC). Стандарт 802.15.14 є базовою основою для більш високорівневих протоколів, таких як ZigBee, WirelessHART і MiWi. Він може бути також використаний спільно зі стандартом 6LoWPAN і стандартними протоколами Інтернету для побудови бездротових сенсорних мереж.

Фізичний рівень 802.15.14 PHY визначає спосіб передачі даних, інтерфейс організації зв'язку, апаратні особливості та параметри, необхідні для побудови мережі. На практиці фізичний рівень управляє роботою трансивера, виконує вибір каналів, сигналів управління і рівня потужності передачі.

У стандарті 802.15.4 на фізичному рівні під обмін даними зарезервовані 27 каналів в трьох частотних діапазонах: 868 МГц, 910 МГц і 2.4 ГГц, що дозволяє використовувати стандарт в неліцензованому в більшості країн світу діапазоні для промислових, наукових і медичних цілей ISM (Industrial Scientific Medical). На території України доступний до використання тільки діапазон 2.4 ГГц.

Перша версія стандарту 802.15.4 визначала два фізичні рівні з широкосмисловою модуляцією з прямим розширенням спектра DSSS (Direct Sequence Spread Spectrum): перший в смузі 868/915 МГц зі швидкістю передачі відповідно 20 і 40 кбіт/с, а другий в смузі 2450 МГц зі швидкістю 250 кбіт/с. У 2006 році допустимі швидкості передачі даних на частотах 868/915 МГц були збільшені до 100 і 250 кбіт/с.

Крім того були визначені чотири специфікації фізичного рівня в залежності від методу модуляції: при збереженні широкосмисловою модуляцією DSSS можливо використанні в діапазоні 868/915 МГц як двійкової, так і квадратурної фазової маніпуляції QPSK (Quadrature Phase Shift Keying). З 2007 року в версію стандарту IEEE 802.15.4a число фізичних рівнів було збільшено до шести за рахунок включення рівня з надширокосмислових радіотехнології UWB (Ultra WideBand) для високошвидкісної передачі даних, а також специфікації рівня з

радіотехнології CSS (Chirp Spread Spectrum), заснованої на розширенні частотного спектра методом лінійної частотної модуляції. Фізичний рівень UWB визначений виділеними частотами в трьох діапазонах: нижче 1 ГГц, 3-5 ГГц і 6-10 ГГц, а для CSS виділений спектр в смузі 2450 МГц неліцензованому діапазону ISM. У 2009 році в версіях стандартів IEEE 802.15.4c і IEEE 802.15.4d були розширені доступні частотні діапазони. Дані специфікації визначають можливість використання на фізичному рівні приймально-передавальних пристроїв з квадратурною фазовою маніпуляцією QPSK або з фазовою маніпуляцією більш високих порядків на частоті 780 МГц, а на частоті 950 МГц - гаусову частотну маніпуляцію GFSK (Gaussian Frequency-Shift Keying) або двійкову фазову маніпуляцію BPSK (Binary Phase-Shift Keying).

На каналному рівні специфікація IEEE 802.15.4 визначає механізми взаємодії елементів мережі на фізичному рівні для забезпечення формування фрагментів даних (кадрів), перевірки та виправлення помилок, відправку кадрів на мережевий рівень. При цьому підрівень MAC каналного рівня регулює множинний доступ до фізичного середовища з поділом за часом, управляє зв'язками трансиверів і забезпечує безпеку. Стандарт IEEE Std 802.15.4 забезпечує двосторонню напівдуплексну передачу даних, підтримуючи при цьому шифрування AES 128. Доступ до каналу заснований на принципі Carrier Sense Multiple Access With Collision Avoidance (CSMA/CA) - багатостанційний доступ з контролем несучої та запобіганням конфліктів. CSMA/CA - це мережевий протокол, в якому використовується принцип прослуховування несучої частоти. Особливістю пристроїв, поєднаних в мережу по стандарту IEEE Std 802.15.4, є низьке енергоспоживання за рахунок переходу трансивера в режим «засинання» при відсутності даних для пересилання і збереження підключення в цьому режимі. При розробці стандарту основний акцент робився на швидкість процесів конфігурації та реконфігурування. Зокрема, перехід приймача в

активний стан триває близько 10-15 мс, а підключення до мережі нових пристроїв від 30 мс. При цьому тривалість реконфігурації та підключення пристроїв залежить від сталості «прослуховування» маршрутизаторами мережі. Стандарт визначає два типи вузлів мережі: 1) повнофункціональний пристрій FFD (Fully Function Device), яке може реалізувати як функцію координації роботи та установки параметрів мережі, так і працювати в режимі типового вузла; 2) пристрій з обмеженим набором функцій RFD (Reduced Function Device), що володіє тільки можливістю підтримки зв'язку з повнофункціональними пристроями. У будь-якій мережі повинен бути, принаймні, один FFD, який реалізує функцію координатора. Кожен пристрій має 64-бітний ідентифікатор, але в деяких випадках для обмеженої області може використовуватися короткий 16-бітний для з'єднань в персональній мережі PAN.

На каналному рівні стандарті IEEE Std 802.15.4 наведені загальні рекомендації до побудови топології мережі. Мережі можуть бути одноранговими P2P (peer-to-peer, point-to-point), або мати топологію «зірка». На основі структури P2P можуть формуватися довільні структури з'єднань, обмежені лише дальністю зв'язку між парами вузлів[10].

2.1.2. Стандарт ZigBee

Як було зазначено вище, стандарт IEEE Std 802.15.4 описує два нижні рівня мережевої моделі OSI, не визначаючи вимог до верхніх рівнів і умов їх сумісності. Рішення цих завдань вимагало розробки спеціальних комунікаційних протоколів. Найбільш відомими є протоколи альянсу ZigBee, якої був створений найбільшими світовими компаніями, що спеціалізуються в області розробки програмно-апаратних засобів для інфокомунікаційних систем. У числі більш ніж двохсот членів альянсу ZigBee, які координують роботи з просування технологій і виробництва

технічних засобів для бездротових сенсорних мереж – Texas Instruments, Motorola, Philips, IBM, Ember, Samsung, NEC, Freescale Semiconductor, LG, OKI та багато інших. Альянс розробив і ратифікував у 2004 році стандарт ZigBee, що включає повний стек протоколів для бездротових сенсорних мереж. Назва специфікації ZigBee походить від Zig-zag - зигзаг і Bee - бджола. Малося на увазі, що топологія мережі буде нагадувати звивисту траєкторію польоту бджоли від квітки до квітки.

Специфікація ZigBee орієнтована на програми, що вимагають гарантованої безпечної передачі даних при відносно невеликих швидкостях і можливості тривалої роботи мережевих пристроїв від автономних джерел живлення (батарей). Вона забезпечує невисоке споживання енергії та передачу даних зі швидкістю до 250 Кбіт/с на відстань до 75 метрів в умовах прямої видимості.

ZigBee базується на стандарті IEEE Std 802.15.4, який описує тільки фізичний рівень і рівень доступу до середовища MAC для бездротових мереж передачі даних з низьким енергоспоживанням. Стандарт ZigBee включає опис мережевих процесів управління, сумісності та профілів пристроїв, а також інформаційної безпеки. На мережевому рівні в ZigBee визначені механізми маршрутизації та формування логічної топології мережі.

Основна особливість технології ZigBee полягає в тому, що вона при малому енергоспоживанні підтримує не тільки прості топології мережі («точка-точка», «Дерево» і «зірка»), а й самоорганізує і самовідновлює складні топології з ретрансляцією і маршрутизацією повідомлень. Крім того, специфікація ZigBee містить можливість вибору алгоритму маршрутизації.

Крім того протоколи ZigBee дозволяють мережевим пристроям перебувати в сплячому режимі більшу частину часу, що істотно збільшує ресурс роботи вузлів при живленні від батарейних джерел. В BSS на основі ZigBee підтримується режим «профілів пристроїв» або профілів для різних

датчиків, які сумісні на рівні стека протоколу і можуть об'єднуватися в мережу, передавати, приймати та ретранслювати інформацію. У той же час розуміти цю інформацію буде тільки той пристрій, для якого вона призначена.

Всі пристрої стандарту ZigBee в залежності від рівня складності поділяються на три класи, вищий з яких - координатор - управляє процесом формування мережі, зберігає дані про її топологію та служить шлюзом для передачі даних, що збирає дані від всіх сенсорів BSS для їх подальшої обробки. У мережі, як правило, використовується тільки один PAN-координатор. Середній за складністю пристрій - маршрутизатор – здатний ретранслювати повідомлення, підтримувати всі топології мережі, а також виконувати функції координатора кластеру. І, нарешті, найбільш простий вузол - термінал – здатний лише передавати дані найближчому маршрутизатору.

Таким чином, стандарт ZigBee підтримує мережу з кластерною архітектурою, сформовану зі звичайних вузлів, об'єднаних в кластери за допомогою маршрутизаторів. Маршрутизатори кластерів запитують сенсорні дані від пристроїв і, ретранслюючи їх один одному, передають координатору, який зазвичай має зв'язок з зовнішньою IP-мережею, куди й відправляє інформацію для накопичення й остаточної обробки.

Мережа ZigBee є самоорганізаційною, тобто всі вузли здатні самостійно визначати і коригувати маршрути доставки даних. Дані передаються за допомогою радіопередавачів від одних вузлів до інших по ланцюжку, і в підсумку найближчі до шлюзу вузли скидають всю акумульовану інформацію на шлюз. Ця інформація включає дані, що зчитуються з сенсорних датчиків, а також дані про стан пристроїв і результатах процесу передачі інформації. У разі виходу частини пристроїв з ладу, робота сенсорної мережі після реконфігурації повинна продовжитися. Бездротові вузли функціонують під управлінням спеціального додатку.

Зазвичай всі вузли сенсорної мережі використовують одну і ту ж керуючу програму, що забезпечує їх функціональність і виконання мережевих протоколів.

Концерн RF4CE (Radio Frequency for Consumer Electronics) спільно з альянсом ZigBee розробив стандартизовану специфікацію ZigBee RF4CE, призначену для використання в побутових дистанційно керованих аудіо/відео пристроях, таких як телевізори, телеприставки і ігрові консолі. Вона має ряд переваг порівняно з існуючими технічними рішеннями для дистанційного керування, включаючи управління роботою в зоні непрямой видимості, функціональність маніпулятора типу "миша" і клавіатури, управління з розпізнаванням жестів і сенсорним введенням, двосторонній зв'язок, більш тривалий час роботи від акумулятора[11].

2.1.3. Стандарт 6LoWPAN

6LoWPAN (IPv6 Low-Power Wireless Personal Area Network) - стандарт, що забезпечує взаємодію малих бездротових мереж з мережами IP по протоколу IPv6 з малим енергоспоживанням. Стандарт розроблений групою IETF і описаний в RFC 4944 і RFC 4919. Технологія використовується в основному для організації мереж датчиків і автоматизації житлового та офісного приміщення з можливістю управління через інтернет, однак може використовуватися й автономно для реалізації простих бездротових мереж датчиків. Передача даних в стандарті 6LoWPAN має на увазі використання субгігагерцового діапазону і забезпечує швидкість передачі від 50 до 200 Кбіт/с на відстань до 800 метрів.

Архітектура мереж 6LoWPAN дещо відрізняється від традиційних архітектур IP-мереж (наявність спеціалізованого комутаційного обладнання, маршрутизаторів, медіа-конверторів) і від сформованих архітектур

бездротових мереж збору даних. Ближче всього до неї знаходиться архітектура WiFi-мереж, хоча і від неї є ряд відмінностей.

Перш за все, мережі 6LoWPAN є підмережами IPv6-мереж, тобто вони можуть взаємодіяти з іншими мережами та вузлами IP-мережі, але не є транзитними для її мережевого трафіку. Мережі 6LoWPAN складаються з вузлів, які можуть також виконувати роль маршрутизаторів (host і router), крім цього в мережі може бути присутнім один або більше так званих граничних маршрутизаторів (edge routers). Участь в маршрутизації НЕ є обов'язковою вимогою для вузла мережі й він може грати роль, аналогічну ролі кінцевого пристрою в мережах ZigBee або пристроїв з обмеженою функціональністю для мереж 802.15.4.

Вузол, здатний виконувати маршрутизацію в межах мережі 6LoWPAN, називається роутером або маршрутизатором. Граничний маршрутизатор відповідає за взаємодію підмережі 6LoWPAN з мережею IPv6, бере участь в процедурі ініціалізації і маршрутизації в підмережі 6LoWPAN, здійснює компресію/декомпресію заголовків.

IPv6 при обміні із зовнішньою мережею, в разі підключення до мережі IPv4 може грати роль шлюзу IPv6↔IPv4. Вузли підмережі поділяють 64-бітний префікс IPv6, який також є частиною мережевої адреси граничного маршрутизатора. Для адресації всередині мережі можна користуватися 64-бітною (MAC-адресою мережевого інтерфейсу) або використовувати стиснення адреси і вкорочену 16-бітну схему адресації (молодші два байти MAC-адреси). Передбачається, що мережева адреса безпосередньо включає адресу мережевого інтерфейсу, це виключає необхідність застосування протоколу визначення мережевих адрес ARP (Address Resolution Protocol).

Ad-hoc-мережа не має підключення до зовнішньої IP-мережі, не має граничного маршрутизатора. Є самоорганізаційною мережею, що використовує стек протоколів 6LoWPAN для організації роботи та передачі даних між вузлами.

Проста 6LoWPAN-мережа підключена до іншої IP-мережі за допомогою одного граничного маршрутизатора. Граничний маршрутизатор може бути підключений до зовнішньої IP-мережі безпосередньо (підключення типу «точка-точка», наприклад, GPRS/3G-модем) або може входити до складу кампусової мережі (наприклад, мережі організації).

Розширена 6LoWPAN-мережа складається з однієї або декількох підмереж, підключених до зовнішньої IP-мережі через кілька граничних маршрутизаторів, підключених до однієї мережі (наприклад, локальна мережа організації). При цьому граничні маршрутизатори в розширеній мережі поділяють один і той же мережевий префікс. Вузли розширеної мережі можуть вільно переміщатися в межах мережі та здійснювати обмін з зовнішньою мережею через будь-який граничний маршрутизатор (зазвичай вибирається маршрут з найкращими показниками якості сигналу - рівень помилок, рівень сигналу).

Взаємодія між вузлами в мережі 6LoWPAN, а також взаємодія з зовнішніми вузлами здійснюється так само, як і в звичайній IP-мережі. Кожен вузол має свій унікальний IPv6-адрес і може приймати і передавати пакети IPv6.

Прикладні протоколи найчастіше використовують бінарний формат даних при роботі з UDP-протоколом в мережах 6LoWPAN. На відміну від TCP/IP-стека, в 6LoWPAN немає підтримки протоколу транспортного рівня TCP - через великі накладні витрати на формування пакетів і через особливості роботи протоколу, які суттєво ускладнюють його застосування в сенсорних бездротових мережах.

Так само як і мережі ZigBee, мережі 6LoWPAN є здатними до самоорганізації. Для цього використовується стандартна техніка мереж IPv6. На базі заданих параметрів стека автоматично встановлюється оптимальна топологія зв'язків між вузлами в мережі.

Оптимальні маршрути визначаються на основі метрик. На відміну від стандартів ZigBee, 6LoWPAN розширює стандартизацію до рівня прикладних задач, паралельно вирішуючи проблеми з інтеграцією невеликих бездротових вузлів в IP-мережі.

Цільові програми стека 6LoWPAN включають в себе досить великі масштабовані мережі з підключенням до IP-мереж (інтернет, інтранет або екстранет)[12].

Незважаючи на хорошу масштабованість, потенційно прозоре управління і легкий доступ до вузлів, 6LoWPAN підходить не для всіх застосувань. Зокрема, поточна версія стандарту стека протоколів вимагає постійної активності маршрутизаторів для коректної передачі даних, що важко в сенсорних бездротових мережах. Проте, ця особливість дозволяє мінімізувати займаний стеком 6LoWPAN обсяг flash-пам'яті в кінцевому пристрої і, отже, мінімізувати вартість мережевого процесора. Основні області застосування стандарту 6LoWPAN: інтелектуальні системи обліку; управління вуличним освітленням; промислова автоматика; логістичні системи, відстеження товарів або об'єктів інвентаризації; комерційні охоронні системи, системи контролю і управління доступом; деякі військові програми.

Деякі області застосувань 6LoWPAN перегукуються з рядом стандартів ZigBee, проте в даному випадку конкуренція відсутня, скоріше - взаємодія і доповнення один одного, особливо в плані інтеграції сервісів, розширення зон дії мережі.

2.1.4. Стандарти Wireless Hart і ISA100.11a

Стандарти промислових бездротових мереж WirelessHART (IEC 62591) і ISA100.11a, як і розглянуті раніше технології ZigBee і 6LoWPAN, є надбудовами над фізичним рівнем стандарту IEEE 802.15.4. Обидва

стандарти мають загальний принцип роботи і конкурують між собою. Конвергенцію WirelessHART і ISA100.11a планувалося здійснити в єдиному стандарті ISA100.12, однак після п'яти років роботи в кінці 2012 року робота над новим стандартом в рамках Міжнародної асоціації автоматизації (ISA) було припинено, оскільки не вдалося вирішити питання про сумісність цих стандартів для бездротових мереж промислової автоматизації. WirelessHART - протокол передачі даних по бездротовій лінії зв'язку, розроблений фондом HART Communication Foundation для передачі даних у вигляді HART-повідомлень в бездротовому середовищі. Вихідний протокол обміну даними HART в провідних мережах був призначений для взаємодії з польовими датчиками на основі розширеного набору простих команд «запит-відповідь», які передаються в цифровому вигляді по двухпроводній лінії з струмом 4-20 мА. Його бездротовий варіант WirelessHART забезпечує передачу даних зі швидкістю до 250 кбіт/с на відстань до 200 м (в межах прямої видимості) при частоті передачі даних в діапазоні 2.4 ГГц. WirelessHART схвалений міжнародною електротехнічною комісією в якості першого міжнародного стандарту бездротового зв'язку промислової автоматизації під номером IEC 62591.

Бездротова мережа WirelessHART складається з трьох основних елементів:

1. Бездротові польові пристрої, підключені до промислового обладнання. Це може бути пристрій з вбудованою провідною технологією WirelessHART або вже наявний встановлений проводний HART-пристрій з адаптером WirelessHART.

2. Шлюзи - забезпечують обмін даними між польовими пристроями і хост додатками, приєднаними до високошвидкісної магістральної або іншої наявної на підприємстві комунікаційної мережі[13].

Адміністратор мережі/менеджер безпеки - відповідає за конфігурування мережі, планування обміну даними між пристроями,

маршрутизацію повідомлень і моніторинг стану мережі. Адміністратор мережі може бути вбудований в шлюз, хост додаток або контролер автоматизації технологічного процесу. Мережа WirelessHART заснована на сумісних з IEEE 802.15.4 радіопередавачах, працюючих в ISM діапазоні 2,4 ГГц. У них використовується технологія широкосмугового сигналу з прямою послідовністю і перемиканням каналів для забезпечення комунікаційної безпеки і надійності, а також технологія синхронізованого множинного доступу з тимчасовим поділом каналів (TDMA) і контрольованою затримкою для зв'язку між пристроями в мережі.

Кожен пристрій в мережі може служити в якості маршрутизатора для повідомлень від інших пристроїв. Іншими словами, пристрій не має необхідності звертатися безпосередньо до шлюзу, він просто передає своє повідомлення на найближчий сусідній пристрій. Це розширює масштаб мережі та забезпечує надлишкові канали передачі даних для підвищення надійності. Адміністратор мережі визначає надлишкові канали на основі часу затримки, ефективності і надійності передачі. Щоб забезпечити відкритість і вільність надлишкових каналів, передача повідомлень по черзі здійснюється по кожному з них.

Схема мережі WirelessHART також дозволяє легко додавати і переміщати пристрої. Пристрій завжди залишається на зв'язку, коли він знаходиться в зоні дії інших пристроїв в мережі.

Для забезпечення гнучкості при різних умовах застосування стандарт WirelessHART підтримує декілька режимів передачі даних, включаючи односпрямовану публікацію значень параметрів технологічного процесу і управління, миттєве повідомлення по виключенню, спеціальний запит/відгук і передача великих наборів даних з автоматичним сегментуванням. Ці можливості дозволяють налаштовувати передачу даних відповідно до виробничих вимог, що знижує енергоспоживання та непродуктивні витрати.

ISA100.11a - стандарт організації промислових сенсорних мереж, мереж датчиків і приводів. Стандарт розроблений Міжнародним товариством з автоматики ISA (International Society of Automation) і схвалений МЕК як загальнодоступної специфікації. В

Нині йде процес схвалення специфікації в якості стандарту. Для передачі промислових даних використовується низькошвидкісний бездротовий зв'язок з використанням елементів з низьким енергоспоживанням. Обмін даними здійснюється на частоті в районі 2,4 ГГц і швидкості близько 250 кбіт / с. В основі архітектури ISA100.11a, як і в протоколі WirelessHART, лежить стандарт IEEE 802.15.4-2006.

ISA100.11a підтримує протоколи Fieldbus Foundation, Profibus-PA і HART, що працюють на рівні додатків. Фактично, він здатний підтримувати кілька кластерів пристроїв, що працюють із зазначеними протоколами. Він також може підтримувати різні типи датчиків (HART, Profibus і ін.) в одному кластері.

Стандарт ISA100.11a використовує топологію мереж датчиків типу «чарункова мережа» або «Зірка». Мережі з топологією типу «чарункова мережа», що виконують безліч перемикань, використовують більше заряду батарей, ніж мережі з топологією типу «зірка», але є більш безпечними. Таким чином, у користувача є вибір і він може віддати перевагу того чи іншого способу побудови мереж, в залежності від розв'язуваних завдань.

Протоколи WirelessHART і ISA100.11a мають багато спільного, тому що за основу взято стандарт IEEE 802.15.4-2006. З метою підвищення надійності бездротових систем для підприємств в обох випадках на фізичному рівні використовується технологія перебудови робочої частоти FHSS (Frequency Hopping Spread Spectrum), а на канальному рівні метод кодового розподілення CDMA замінений на метод тимчасового поділу TDMA .

Обидва стандарти в останніх версіях підтримують мову опису електронних пристроїв EDDL (Electronic Device Description Language) для забезпечення сумісності польових пристроїв від різних виробників[14].

На прикладному рівні моделі OSI в ISA100.11a для проектування додатків використовується концепція об'єктно-орієнтованої моделі, а Wireless Hart - командно-орієнтована. У ISA100.11a на прикладному рівні хоста введений додатковий підшар для управління UAP і між UAP, який за стандартом ISA для польових шин IEC 61158 розглядається окремо від моделі OSI. У Wireless Hart таке поняття відсутнє. ISA100.11a є повноцінним і перспективним стандартом з технологічної точки зору. Він заснований на відкритих стандартах, а не власних технологіях. Наприклад, він підтримує протокол IPv6 комітету IETF в бездротових персональних мережах низької потужності (6LoWPAN). Адресація пристроїв IPv6 дозволяє використовувати тисячі датчиків і спростити їх підключення при переході до інтернету речей.

Хоча бездротова система ISA100.11a повністю усуває необхідність використання WirelessHART, на даний момент більше 15-ти виробників підтримують стандарт WirelessHART (IEC 62591), тоді як підтримка стандарту ISA100.11a обмежена всього трьома виробниками. Слід також зазначити, що більш дешева технологія ZigBee може бути застосована для домашніх та офісних автоматизацій, в той час як дорогі технології WirelessHART і ISA 100.11a призначені для мереж промислової автоматизації.

2.1.5. Стандарт Z-Wave

Z-Wave - це перший відкритий бездротовий стандарт домашньої автоматизації (Системи «розумний будинок»), в основі якої лежить сітчаста мережа. Він заснований на специфікації ITU G.9959 і визначає всі аспекти взаємодії пристроїв, що підтримують цей протокол, а також забезпечує їх

сумісність. Технологія використовує малопотужні і мініатюрні радіочастотні модулі, які вбудовуються в побутову електроніку і різні системи, такі як освітлення, опалення, контроль доступу, розважальні системи і побутову техніку.

На відміну від Wi-Fi і інших стандартів передачі даних IEEE 802.11, призначених в основному для великих потоків інформації, стандарт Z-Wave працює в діапазоні частот до 1 ГГц і оптимізований для передачі простих керуючих команд (Наприклад, включити/виключити, змінити гучність, яскравість і т.д.). вибір низького радіочастотного діапазону для Z-Wave обумовлюється малою кількістю потенційних джерел перешкод (на відміну від завантаженого діапазону 2,4 ГГц, в якому доводиться вдаватися до заходів, що зменшують можливі перешкоди від працюючих різних побутових бездротових пристроїв - Wi-Fi, ZigBee, Bluetooth).

Також іншими перевагами стандарту можна відзначити мале споживання енергії, низьку вартість виробництва і вбудовування модулів Z-Wave в різні побутові пристрої.

Швидкість передачі даних в мережі становить 9,6 кбіт / с або 40 кбіт / с з повною сумісністю. Використовується модуляція GFSK. Радіус дії приблизно 30 метрів в умовах прямої видимості, в приміщенні зменшується в залежності від форми і матеріалу стін, а також від виду антени.

У мережі Z-Wave вузли діляться на три типи: контролери (Controlllers), маршрутизуючі виконавчі механізми (Routing Slaves) і виконавчі механізми (Slaves). У реальній мережі всі типи пристроїв можуть працювати в будь-якій комбінації.

Z-Wave використовує сітчасту топологію мережі з маршрутизацією повідомлень від джерела і має один основний контролер і нуль або більше вторинних контролерів, які керують маршрутизацією і безпекою. У мережі Z-Wave кожен вузол або пристрій може приймати і передавати керуючі сигнали інших пристроїв мережі, використовуючи проміжні сусідні вузли.

Це самоорганізована мережа з маршрутизацією, залежною від зовнішніх факторів - наприклад, при виникненні перешкоди між двома найближчими вузлами мережі, сигнал піде через інші вузли мережі, що знаходяться в радіусі дії.

Таким чином, Z-Wave мережа може мати радіус передачі набагато більший, ніж дальність передачі одного вузла. Однак через велику кількість приймання може бути отримана невелика затримка між командою управління і бажаним результатом. Для того щоб Z-Wave пристрої мали можливість маршрутизувати дані ними, вони не можуть перебувати в сплячому режимі. Таким чином, пристрій без окремого живлення батарейок не призначені в якості пристроїв ретрансляції. Мережа Z-Wave може включати до 232 пристроїв з можливістю розширення мережі, якщо потрібно ще кілька пристроїв. Додаткові пристрої в мережу можуть бути додані в будь-який час, так само як і кілька керуючих контролерів[15].

Хоча технологія Z-Wave є простим і дешевим рішенням, низька швидкість передачі даних виключає передачу зображень, звуку і високошвидкісних даних. Крім того, для рішень, де потрібно більше 30 пристроїв, Z-Wave-система є більш дорога, ніж кабельні системи. Через свої конструктивні особливості, такі системи мають обмежені масштаби і радіус дії, і вимагають використання повторювачів або навіть кабельні з'єднання.

2.1.6. Стандарт Bluetooth Low Energy

Технологія Bluetooth Low Energy (BLE) - є технологією бездротового зв'язку для ближніх комунікацій, розробленої групою Bluetooth Special Interest Group (SIG). На відміну від попередніх стандартів - Bluetooth 2.0, Bluetooth 2.1 + EDR, Bluetooth 3.0, стандарт BLE з самого початку орієнтований на застосування в системах збору даних, моніторингу з автономним живленням. BLE споживає в 10-20 разів менше енергії і здатний

передавати дані в 50 разів швидше, ніж класичні Bluetooth-рішення. На відміну від технологій сенсорних мереж, таких як, ZigBee, 6LoWPAN або Z-Wave, орієнтованих на розгалужені розподілені мережі з численними передачами даних між вузлами мережі, стандарт Bluetooth Low Energy розрахований на топології типу «точка-точка» і «зірка». Основними областями застосування BLE є пристрої забезпечення безпеки, управління електроприладами і відображення показань, датчики на батарейках, домашні медичні прилади, спортивні тренажери. Пристрої BLE працюють в діапазоні 2,4 ГГц. У стандарті визначено 40 частотних каналів з відстанню в 2 МГц між каналами. На фізичному рівні застосована GFSK-модуляція (Gaussian Frequency Shift Keying) з індексом модуляції в межах від 0,45 до 0,55, що дозволяє зменшити пікове споживання енергії. Швидкість передачі на фізичному рівні 1 Мбіт / с. У стандарті BLE чутливість приймача визначена як рівень сигналу на приймачі, при якому частота бітових помилок BER (Bit Error Rate) досягає рівня 10⁻³. Вона повинна становити -70 дБм або краще. Технологія адаптивної стрибкоподібної перебудови частоти, яка використовується в BLE, дає їм змогу швидко змінювати робочу частоту в широкому діапазоні робочих частот. Це не тільки дозволяє знизити інтерференцію, а й зменшити або повністю уникнути переповнення в робочому частотному діапазоні. Поряд з широкомовною режимом, BLE пропонує спосіб передачі даних, орієнтований на встановлене між окремими пристроями з'єднання. Як і класичний стек протоколів Bluetooth, стек BLE складається з двох основних частин: контролера (controller) і вузла мережі (host) (рис. 5.15). Контролер включає в себе фізичний і канальний рівень і часто реалізується у вигляді системи-на-кристалі з інтегрованим бездротовим трансивером. Частина стека, іменована вузлом мережі, реалізується програмно на мікроконтролері додатків і включає в себе функціональність верхніх рівнів (рис. 5.15): протокол адаптації L2CAP (Logical Link Control and Adaptation Protocol), протокол атрибутів ATT

(Attribute Protocol), протокол атрибутів профілів пристроїв GATT (Generic Attribute Profile), протокол забезпечення безпеки SMP (Security Manager Protocol), протокол забезпечення доступу до функцій профілю пристроїв GAP (Generic Access Profile). Взаємодія між верхньою і нижньою частинами стека здійснюється через інтерфейс HCI (Host Controller Interface). Додаткова функціональність прикладного рівня може бути реалізована поверх рівня вузла мережі.

Незважаючи на те, що деякі функції контролера BLE запозичені у класичного Bluetooth, вони не сумісні між собою, тобто пристрій, що підтримує тільки BLE (однорежимні пристрій - single-mode device) не зможе взаємодіяти з пристроєм, що підтримує тільки Bluetooth версій 2.x / 3.0. Для здійснення взаємодії між ними хоча б один з пристроїв має підтримувати обидва стека протоколів (дворежимні пристрій - dual-mode device). однорежимні пристрої володіють найменшим енергоспоживанням і в основному являють собою кінцеві виконавчі пристрої. Дворежимні пристрої припускають можливість періодичного отримання енергії, розташовуються на різних мобільних пристроях, а також можуть функціонувати і як звичайні Bluetooth-пристрої[16].

Безумовно, велика частина областей застосування Bluetooth може бути успішно замінена або доповнена пристроями BLE, що продовжить термін служби пристроїв за рахунок більш ефективного управління енергоспоживанням. Зокрема, можливе застосування дворежимних пристроїв BLE в мобільних телефонах, планшетних комп'ютерах, ноутбуках. Однорежимні пристрої можуть застосовуватися в якості бездротового інтерфейсу датчиків на батарейках, що застосовуються як окремо, так і в складі інших пристроїв - в годиннику, пульсометра, крокомір, домашніх тонометрах, термометрах і тому подібних пристроїв. У складі мобільних пристроїв BLE може бути використаний для управління домашньою автоматикою, пристроями освітлення або охорони, як мінімум, в межах

одного приміщення. Для керування пристроями в межах всього будинку можливе використання BLE в якості шлюзу між керуючим пристроєм і мережею домашньої автоматики. Низький рівень споживання енергії та більш стійка робота в умовах великої кількості аналогічних пристроїв в ряді випадків дозволяє розглядати BLE як альтернативу пристроїв NFC, зокрема RFID-мітками. Але більш цікавий варіант використання BLE спільно з NFC. У цьому випадку перші забезпечують більший радіус стійкої роботи і велика кількість спільно діючих механізмів, а другі служать для встановлення логічного з'єднання між парою пристроїв, забезпечуючи більш високий рівень безпеки за рахунок меншого радіуса дії[17].

2.1.7. Сімейство стандартів IEEE 802.11

IEEE 802.11 - набір стандартів зв'язку для реалізації бездротових локальних мереж в різних частотних діапазонах. Користувачам більше відомий за назвою Wi-Fi (від англійського словосполучення Wireless Fidelity, яке можна дослівно перекласти як «висока точність безпроводної передачі даних»), що є торговою маркою об'єднання Wi-Fi Alliance. Wi-Fi - один з найпопулярніших груп стандартів і повсюдно використовується для організації домашніх і офісних мереж, публічного доступу до Інтернету в готелях, кафе, магазинах і в інших публічних місцях. Набув широкого поширення завдяки використанню в мобільних пристроях, КПК і ноутбуках. Як і у всіх технологій сімейства 802, технологія 802.11 визначається двома нижніми рівнями, тобто фізичним рівнем і рівнем MAC, а рівень LLC виконує свої стандартні загальні для всіх технологій LAN функції. На фізичному рівні існує кілька варіантів специфікацій, які відрізняються використанням частотним діапазоном, методом кодування і як наслідок - швидкістю передачі даних. Всі варіанти фізичного рівня працюють з одним і

тим же алгоритмом рівня MAC, але деякі тимчасові параметри рівня MAC залежать від використовуваного фізичного рівня.

Рівень MAC виконує в бездротових мережах більше функцій, ніж в дротяних. Функції рівня MAC в стандарті 802.11 включають:

- доступ до середовища;
- забезпечення мобільності станцій при наявності декількох базових станцій;
- забезпечення безпеки.

У мережах 802.11 рівень MAC підтримує два режими доступу до середовища: розподілений режим DCF (Distributed Coordination Function) і централізований режим PCF (Point Coordination Function). Режим PCF застосовується в тих випадках, коли необхідно пріоритезувати чутливий до затримок трафік.

Спочатку стандарт IEEE 802.11 припускав можливість передачі даних по радіоканалу на швидкості не більше 1 Мбіт/с і опціонально на швидкості 2 Мбіт/с. Один з перших високошвидкісних стандартів бездротових мереж IEEE 802.11b використовує кодування за допомогою комплементарних кодів ССК (Complementary Code Keying).

Робочий діапазон стандарту - 5 ГГц. Використовується мультиплексування з ортогональним частотним поділом каналів OFDM (Orthogonal frequency-division multiplexing).

Стандарт IEEE 802.11g передбачає використання діапазону частот 2,4 ГГц, забезпечуючи швидкість з'єднання до 54 Мбіт / с. Крім того, він гарантує зворотну сумісність зі стандартом 802.11b. Зворотна сумісність стандарту IEEE 802.11g може бути реалізована в режимі модуляції ССК, і тоді швидкість з'єднання буде обмежена 11 Мбіт / с або в режимі модуляції OFDM, при якому швидкість може досягати 54 Мбіт / с.

Стандарт IEEE 802.11n теоретично здатний забезпечити швидкість передачі даних до 600 Мбіт / с, застосовуючи передачу даних відразу по

чотирьом антенам. При роботі по одній антені - швидкість до 150 Мбіт/с. Пристрої 802.11n працюють в діапазонах 2,4-2,5 або 5,0 ГГц.

Пристрої 802.11n можуть працювати в трьох режимах:

1. успадкованому (Legacy), в якому забезпечується підтримка пристроїв стандартів 802.11b / g і 802.11a;
2. змішаному (Mixed), в якому підтримуються пристрої 802.11b / g, 802.11a і 802.11n;
3. чистому - в цьому режимі реалізуються і підвищена швидкість і збільшена дальність передачі даних.

Існує також стандарт IEEE 802.11p - технологія, розроблена для бездротової передачі інформації між високошвидкісними транспортними засобами і об'єктами транспортної інфраструктури з метою створення інтелектуальної транспортної системи в рамках концепції інтернету речей. Використовуваний частотний діапазон - 5.9 ГГц (5.85-5.925 ГГц).

З складу стандарту IEEE 802.11 входить також технологія IEEE 802.11s, яка дозволяє організувати ієрархічні бездротові ad-hoc мережі з мобільними і статичними вузлами (mesh-мережі), розширює функціональність бездротового доступу в Інтернет і дозволяє реалізовувати точки доступу з охопленням на порядок вищим, ніж у звичних хот-спотів[18].

Крім цього зараз розробляється стандарт IEEE 802.11ac для бездротових локальних мереж, що працює на частотах 5-6 ГГц. Максимальна теоретична пропускна здатність в IEEE 802.11ac становить 6933,3 Мбіт / с і забезпечується при ширині каналу 160 МГц і умови використання 8 антен MU-MIMO (Multi-User Multiple-Input / Multiple-Output), що працюють в режимі просторового мультиплексування. Це еквівалентно поділу потоку даних на кілька просторових потоків beamforming (від англ. «Формування променя» - технологія формування адаптивної діаграми спрямованості антени) і передачі їх одночасно за допомогою кількох антен.

Енергоспоживання в порівнянні з 802.11n знижено до 6 разів. Реалізована зворотна сумісність з 802.11a/b/g/n.

2.1.8. Стандарт DECT ULE

DECT ULE (Digital European Cordless Telecommunications Ultra Low Energy) – бездротова технологія з низьким енергоспоживанням, яка підтримує як традиційну телефонію, так і пакетну передачу даних на низьких швидкостях. DECT ULE є розвитком стандартної технології бездротового телефонного зв'язку DECT.

Поява доповнення DECT ULE покликана забезпечити роботу різних пристроїв з низьким енергоспоживанням і низькою пропускну здатністю, таких, як сенсорні пристрої, розумні лічильники, пристрої автоматизації будинку і ін. DECT ULE перейняв багато позитивних властивостей технології DECT, додавши до них нові можливості, включаючи велику дальність дії, високу стійкість перед перешкодами, зарезервованій під усі світові діапазони частот, низьку вартість, низьке енергоспоживання, можливість співіснування з іншими технологіями (Wi-Fi, Bluetooth і ін.), можливість виходу в інші мережі через стандартизований протокол, зрілість технології. Однією з головних особливостей DECT ULE є підтримка протоколу IPv6, що дозволяє використовувати цей стандарт в Інтернеті речей.

DECT ULE вперше був затверджений в 2011 р і в цьому ж році з'явилися перші продукти. Як і DECT, стандарт DECT ULE працює в діапазоні 1,88-1,90 ГГц (в Європі), тому він має більшу завадостійкість, ніж ZigBee, Bluetooth, Wi-Fi, які працюють в діапазоні 2,4 ГГц.

Швидкість передачі даних - до 1 Мбіт / с. Дальність роботи становить 600 метрів на відкритому просторі і близько 70 метрів всередині приміщень.

Тривалість роботи пристроїв DECT ULE від батарейок вимірюється роками (від 4 до 10 років).

Архітектура стека протоколу DECT ULE показана на рис. 5.17. фізичний рівень працює на частотах 1880-1920 МГц з символічною швидкістю 1,152 Мбіт/с. Для радіодоступу використовуються технології FDMA / TDMA / TDD. Мережі DECT ULE в основному будуються по топології «Зірка» з одним керуючим пристроєм. Рівень доступу до середовища MAC підтримує традиційний стандарт DECT і всі пов'язані з ним можливості з пошуку пристроїв, встановлення з'єднань, безпеки та ін. Управління даними на канальному рівні DECT ULE DLC (Data Link Control) забезпечує мультиплексування і сегментацію великих пакетів з верхніх рівнів. Також цей стандарт забезпечує аутентифікацію і шифрування даних, цілісність пакетів і їх послідовну доставку з найкращим можливим якістю (best effort).

Стек DECT ULE встановлює постійний віртуальний канал PVC (permanent virtual circuit) для рівня додатків і забезпечує підтримку широкого спектру різних протоколів. Однією з можливих технологій для зв'язку між керуючим пристроєм і терміналом DECT ULE є 6LoWPAN.

Стек DECT ULE може бути розділений на площину управління (C-plane) і площину користувача (U-plane). Передбачається, що рівень адаптації ULE 6LoWPAN може працювати безпосередньо на рівні DLC площині користувача.

Прикладний протокол CoAP (Constrained Application Protocol), який представляє собою двійкову версію протоколу http, спрощену під завдання транспортування даних по лініях з обмеженою пропускнуою спроможністю, також може бути використаний в DECT ULE мережах з підтримкою протоколу IPv6[19].

2.1.9. Протокол MQTT

Наявні протоколи для Web-послуг на базі протоколу HTTP не відповідають вимогам у контексті послуг IoT і M2M і потребують доопрацювання. Крім того, потрібно розробити нову, більш вільно пов'язану архітектуру міжплатформного ПО, яка дозволить подолати обмеження таких моделей взаємодії як SOA, REST, Pub / Sub.

Ці проблеми повинен вирішити протокол передачі телеметричних повідомлень по черзі MQTT (Message Queuing Telemetry Transport) - легкий і простий протокол обміну повідомленнями, призначений для зв'язку комп'ютеризованих пристроїв, підключених до локальної або глобальної мережі, між собою і різними громадськими чи приватними веб-сервісами. Його завдання - замінити пропрієтарні технології, використовувані різними компаніями і стати таким же стандартом обміну даними в мережі Інтернет, як протокол HTTP. Протокол MQTT спочатку був створений для датчиків, які відстежують стан труб, проте пізніше сфера його діяльності була розширена і він знайшов своє застосування у безлічі вбудованих рішень, в тому числі в смартфонах. Так соціальна мережа Facebook застосовує цей протокол для обміну повідомленнями (Facebook Messenger).

У мережі на базі протоколу MQTT розрізняють 3 об'єкти:

- 1) видавець (publisher) - MQTT-клієнт, який при виникненні певних подій передає інформацію про нього в брокер;
- 2) брокер (broker) - MQTT-сервер, який приймає інформацію від видавців і передає її відповідним передплатникам, в складних системах може виконувати також різні операції, пов'язані з аналізом і обробкою даних, що надійшли;
- 3) передплатник (subscriber) - MQTT-клієнт, який після підписки у відповідного брокера більшу частину часу «слухає» його і постійно готовий до приймання та обробки вхідного повідомлення від брокера.

Специфікація MQTT відкрита і доступна в Інтернеті. В даний час є два варіанти специфікації MQTT: MQTT v3.1 - основна специфікація для мереж на базі TCP / IP і MQTT-S v1.2 для датчиків і вбудованих пристроїв в мережах, відмінних від TCP / IP, наприклад ZigBee.

Поки що неясно, який радіоспектр буде використовуватися для нового протоколу, але планується, що сам пристрій має бути досить економічним, енергоефективним, щоб працювати тривалий час від заряду акумулятора. MQTT вже використовується в роботі супутників, а також в медицині та деяких промислових сферах. Основні переваги протоколу MQTT: невеликі накладні витрати на транспортному рівні (заголовок фіксованого розміру довжиною 2 байт); протокол обміну зведений до мінімуму для зменшення мережевого трафіку; вбудований механізм контролю з'єднання.

Протокол MQTT має ряд переваг, порівняно з протоколом HTTP: менші накладні витрати на передачу даних і менша смуга пропускання. Для своєї роботи він не вимагає постійного з'єднання між клієнтом і сервером (як у випадку HTTP). MQTT також добре адаптований до роботи по каналах зв'язку з низькою пропускнуою здатністю.

Як було зазначено вище, протокол MQTT забезпечує обмін повідомленнями в режимі «публікація/підписка», який дає їм змогу надсилати і отримувати дані і сигнали тривоги, коли виникає деяка подія (Event-driven application). У моделі з одним видавцем і багатьма передплатниками можна відправляти інформацію з однієї точки багатьом іншим пристроям або «слухачам», які зацікавлені в отриманні інформації. Це схоже на концепцію соціальної мережі, коли одна людина розміщує інформацію, а багато абонентів одночасно переглядають її. Вбудовані пристрої можуть використовувати протокол MQTT для збору даних від декількох пристроїв з обмеженою пропускнуою спроможністю і надання інформації багатьом передплатникам. В результаті система є відносно проста

для настройки і надає ідеальний комунікаційний мережевий протокол для хмарних рішень в області IoT[20].

2.2. Керування даними в програмно-апаратних рішеннях для систем управління потоками

Інтернет речей іноді трактують як синонім систем smart (в перекладі з англ. - розумний): розумні пристрої, розумні будинки, розумне місто, розумні підприємства і т.д. Далі розглянемо їх докладніше.

2.2.1. Розумна планета

Окремі масштабні проекти в напрямку створення «розумної» планети, свого роду «інтранет речей», енергійно розвиваються в останні роки. Так, Національне управління США з аеронавтики і дослідженню космічного простору (National Aeronautics and Space Administration, NASA) за підтримки компанії Cisco створює систему глобального збору даних про Землю - «Шкіру планети» (Planetary skin). Планується розробити онлайнову платформу для збору і аналізу даних про екологічну ситуацію, що надходять від космічних, повітряних, морських і наземних датчиків, розкиданих по всій нашій планеті. Ці дані стануть надбанням широкої громадськості, урядів і комерційних організацій. Вони дозволять в режимі, близькому до реального часу, вимірювати, доповідати і перевіряти екологічні дані, своєчасно розпізнавати глобальні кліматичні зміни і адаптуватися до них. Розробка платформи почалася з серії пілотних проектів, включаючи проект Rainforest Skin (букв. - «шкіра тропічних джунглів»), в ході якого буде досліджено процес знищення тропічних лісів в світовому масштабі.

В рамках програми Planetary Skin розробляються системи підтримки прийняття рішень, що дозволяють ефективно управляти такими природними

ресурсами, як біомаса, вода, земля і енергія, кліматичними змінами і пов'язаними з ними ризиками (такими як підйом рівня світового океану, посухи та епідемії), а також розвитком нових екологічних ринків, утворених навколо вуглеводнів, води і біологічного різноманіття.

Концепцію «розумної планети» Smart Planet пропагує компанія IBM. Суть її полягала в тому, що завдяки технологіям IoT можна зробити планету розумніше. Сьогодні вплив цієї ідеї вже помітно відчувається по всьому світу в різних секторах і галузях, а також у нашому повсякденному житті. Компанії, що працюють в сфері енергетики та енергопостачання, знаходять кращі, більш ефективні способи вироблення і розподілу електроенергії. Міста впроваджують рішення для управління дорожнім рухом, що допомагають суспільству заощадити час і гроші і при цьому підвищити якість життя. Компанії, що виробляють споживчі товари, використовують інтелектуальні технології для створення і поставки більш якісних продуктів в більш короткі терміни і за нижчою ціною. Системи охорони здоров'я використовують інформацію для зменшення числа помилок, скорочення витрат і забезпечення більш індивідуалізованого обслуговування[21].

Технології IoT на базі сенсорних мереж широко використовуються в екології, наприклад, відстеження руху птахів, дрібних тварин і комах, моніторинг стану навколишнього середовища з метою виявлення її впливу на сільськогосподарські культури і худобу, виявлення лісових пожеж, повеней, забруднень та ін.

Починати будувати «розумну планету» потрібно з побудови «розумних будинків», об'єднуючи їх потім в «розумні міста», і продовжувати цей процес до тих пір, поки «цифровою інтелектуальністю» не буде наділена вся планета. Ці та інші «розумні» напрями впровадження Інтернету речей розглянуті далі в розділі.

2.2.2. Розумне місто

В останні роки в містах інтенсивно створюються інформаційні системи для автоматизації окремих сфер міського життя: безпеки міського середовища, транспорту, енергетики і ЖКГ, охорони здоров'я, освіти, державного і муніципального управління та ін. Принципи і технології IoT дозволяють створити повнозв'язне інтегроване рішення, необхідне для функціонування міського середовища і доступне всім жителям міста, співробітникам міських служб, чиновникам і керівникам різних рівнів.

Слід визнати, що Інтернет речей поки що не проник глибоко в елементи міської інфраструктури та господарства, але вже сформував сферу впливу, в рамках якої грає практично революційну роль. Це в першу чергу транспорт, енергетика та комунальні послуги, екологія, контроль злочинності, інформаційне забезпечення жителів міста і інтерактивне управління домогосподарством.

Інтелектуальні мобільні пристрої і високошвидкісні територіально розподілені мережі для доступу до них, сенсори, що вбудовуються в міське середовище, - все це забезпечує основу для створення всеосяжних міст (ubiquitous city), або u-міст, в яких об'єкти інфраструктури і люди тісно пов'язані. Уряду декількох країн вже прийняли масштабні програми створення інтелектуальних міст U-City.

Збір інформації від автобусів, обладнаних системою GPS або ГЛОНАСС, дозволяє створювати інтерактивні табло, онлайн-ресурси і додатки, які інформують жителів про те, скільки їм доведеться чекати автобуса. Інший цікавий приклад - розумні сміттєві контейнери. Сигнал про наповнення подається в централізовану систему управління, яка відстежує на карті всі сміттєзбиральні машини і включає наповнений контейнер в маршрут найближчого вантажівки. І це теж вже не фантастика: саме так працює сміттєзбиральна система в Дубліні і Барселоні[22].

2.2.3. Розумний будинок

«Розумний будинок» призначений для максимально комфортного життя людей за допомогою використання сучасних високотехнологічних засобів.

Принцип роботи системи:

«Розумний дім» полягає в автоматизації всього, з чого складається житлова споруда: освітлення, кондиціонування, система безпеки, електроенергія, опалення, водопостачання та водовідведення і так далі. До основних підсистем «розумного будинку» відносяться: клімат-контроль, освітлення, мультимедіа (аудіо і відео), охоронні системи, зв'язок і інші.

У стандартному проекті «розумного будинку» можна виділити три основні підмережі: мережа мультимедійних пристроїв, мережа електроосвітлювального обладнання і сенсорну мережу. В останньому випадку це датчики руху, світла, температури, тиску, вологості, вібрації і т.п. Таким чином, «розумний дім» складається з програмного і апаратного забезпечення, датчиків і провідної/ бездротової мережі.

У загальному випадку, «розумний дім» надає його власнику такі переваги:

- 1) зниження споживання ресурсів (газ, вода, електроенергія);
- 2) високий рівень комфорту;
- 3) забезпечення необхідної взаємодії всіх автоматизуються систем об'єкта нерухомості, завдання різних режимів роботи;
- 4) зниження ймовірності виникнення аварійних ситуацій;
- 5) підвищення оперативності, простоти і зручності управління.

Для автоматизації будинку смарт-вузли можуть бути інтегровані безпосередньо в побутових пристроїв, наприклад в пилососи, мікрохвильові печі, холодильники і телевізори (що описуються далі). Вони можуть взаємодіяти один з одним і з зовнішньою мережею через інтернет. Це

дозволить кінцевим користувачам легко управляти пристроями будинку як локально, так і віддалено[23].

Більшість побутових пристроїв з категорії «розумних» речей можна поділити на дві групи за типом використання інтернету.

До першої групи належить техніка, яка через WWW оновлює своє програмне забезпечення, отримує нові функції, приймає сигнали від знаходиться далеко господаря, і, відповідно, відправляє йому інформацію, яка підтверджує виконані дії та свій стан. Цей тип використання інтернету побутовою технікою є найбільш розумним і здатний довести потенційному споживачеві свою корисність.

До другої групи входить техніка, в якій інтернет є як би стороннім тілом. Суть рішення в тому, що в абсолютно звичний побутовий прилад, типу мікрохвильовки або холодильника, вбудовується спрощений комп'ютер і дисплей, після чого з їх допомогою можна отримувати мультимедійні розваги там, де їх раніше не було, наприклад, на тій же кухні.

Одним з найперших прикладів побутової техніки, що має підключення до Інтернету, є звичайний тостер, оснащений інтерфейсом для віддаленого включення і повідомлення про готовність підсмаженого тосту. Так техношутка Джона Ромки, одного з перших фахівців в області TCP/IP-протоколу, породила в далекому 1988 році технотренд Інтернету речей, який в наші дні втілюється в життя. Нижче наведені найбільш характерні приклади «розумних» домашніх речей з підключенням до інтернету.

Інтернет-холодильник (Internet refrigerator або Smart refrigerator) - новий клас побутових холодильників, що з'явився на початку XXI століття. Як правило, він має вбудований комп'ютер з постійним підключенням до мережі інтернет і сенсорний екран на фронтальній панелі (рисунок 2.1). Такий холодильник не тільки зберігає продукти, а й дає можливість користуватися інтернетом, через який можна отримати доступ до різних сайтів (наприклад, з кулінарними рецептами для приготування страв) і навіть

замовляти продукти в інтернет-магазинах з доставкою додому. Крім того, за допомогою інтернет-холодильника можна спілкуватися, використовуючи електронну і відеопочту. Інтернет-холодильник може надавати цілий ряд сервісів: доступ в Інтернет, відеотелефон, e-mail, TV, MP3- музику, базу даних по кулінарних рецептах і правилам харчування, електронне перо, щоб залишити повідомлення, голосові послання. Ряд моделей інтернет-холодильників обладнані радіоприймачами. Крім того, при використанні інтернет-холодильника з'являється можливість вивести на екран картинку з веб-камери зовнішнього відеоспостереження. Це дозволяє бачити те, що відбувається у дворі приватного будинку, навіть не покидаючи кухні, доглядати за своїм малюком, що знаходяться в дитячій кімнаті і т.д. Деякі пристрої даного типу також можуть стежити за вмістом холодильника, вибираючи оптимальні умови зберігання та заморозки продуктів. Крім цього, інтернет-холодильник відстежує продукти з терміном придатності. Інформація про все це надходить на смартфон користувача і останній, перебуваючи в магазині, може оцінити свої реальні потреби в продуктах.



Рис. 2.1 Приклад Інтернет-холодильнику

Робот-пилосос може діяти автономно, програмуватися і управлятися через Інтернет, для чого є ряд сенсорів і інфрачервона вбудована камера (рисунок 2.2). Система управління роботою пилососа робить кілька знімків в

секунду створюючи, таким чином, карту всього будинку або окремих його кімнат. Пристрій також має можливість запам'ятовувати оптимальний шлях збирання і визначати своє місцезнаходження в будинку. Акумулятора вистачає на певний час збирання (зазвичай до 1,5 годин), після закінчення якого робот сам відправляється на підзарядку. До пилососа є бездротовий доступ Wi-Fi за допомогою комп'ютера або смартфона. Через ці пристрої можна запустити його і в режимі реального часу спостерігати за тим, що відбувається в кімнаті. Більш того, можна поговорити з людьми, які знаходяться в будинку через систему голосового зв'язку. Вбудований джерело світла дозволяє бачити в повній темряві і перевірити приміщення навіть вночі.



Рис. 2.2 Приклад робота-пилососа.

Інтернет мікрохвильова піч має вбудований модем для виходу в інтернет, пам'ять для зберігання завантажувати інформацію і пульт управління. Вона виконує такі завдання: скачування рецептів з інтернету і самопрограмування; зв'язок з компаніями-виробниками продуктів; дає доступ до системи замовлення продуктів по інтернету.

Інтернет-кондиціонер підключається до інтернету по дротову або бездротову мережу WiFi і дає користувачеві доступ до управління кондиціонером з будь-якої точки земної кулі. Власник може дистанційно вмикати і вимикати систему, програмувати настройки, вибір між режимами, температуру, швидкість вентилятора, задавати параметри, словом здійснювати будь-які маніпуляції, доступні зі звичайного пульта. Керувати

таким кондиціонером можна з будь-якого пристрою (комп'ютер, ноутбук, планшет, смартфон), в якому встановлена спеціальна програма і який має вихід в інтернет[24].

Система по догляду за домашніми тваринами покликана забезпечити їм всі необхідні комфортні умови існування. Така система використовується в разі тривалої відсутності господарів будинку - це дозволяє не турбуватися про добробут своїх домашніх улюбленців. Основними завданнями системи по догляду за домашніми тваринами є автоматична подача їжі і пиття, а в разі виникнення непередбачених обставин - інформування господарів про них (по телефону, за допомогою SMS або по електронній пошті). За бажанням можна скласти повний звіт про поведінку домашніх улюбленців під час відсутності господарів - скільки разів і коли їли, коли ходили в туалет, пили воду і т.д. Можна навіть супроводити цей звіт фотографіями (якщо встановлена камера спостереження) і передавати їх (по електронній пошті, за допомогою MMS) - словом, все, щоб господарі відчували себе комфортно і були впевнені в тому, що їх улюбленцям нічого не загрожує.

2.2.4. Розумна енергія

В даний час найбільш опрацьованим варіантом застосування технологій IoT є «розумні мережі» (Smart Grids) в енергетиці. Робота такої мережі заснована на тому, що постачальник і споживач отримують об'єктивну картину по використанню енергоресурсів за рахунок моніторингу на всіх ділянках мережі і, як наслідок, отримують можливість оперативного управління. У разі аварій такі мережі здатні автоматично ідентифікувати проблемні ділянки і протягом короткого часу робити електроенергію по резервним схемам, відновлюючи електропостачання для споживачів.

«Розумні» мережі означають можливості за гнучким регулювання споживання електроенергії, як у «ручному», так і в автоматичному режимі.

Управління енергомережею проводиться за допомогою наступних систем:

«Розумної» маршрутизації енергопотоків (Smart Routing) - системи контролю навантаження і якості, самовідновлення мереж в результаті аварійних подій, зберігання енергії та ін .;

«Розумних» вимірювань (Smart Metering) - сучасні інтелектуальні прилади обліку (Smart Meter), системи інтелектуальної будівлі (Smart Home), «розумні» побутові прилади.

«Розумний» (або інтелектуальний) лічильник (Smart Meter) - прилад обліку енергоресурсів з розширеними можливостями, який дозволяє контролювати величину спожитих енергоресурсів і періодично передавати інформацію через телекомунікаційну мережу постачальника енергоресурсів або в центр обліку та розрахунків за житлові та комунальні послуги. «Розумні» лічильники можуть вимірювати витрату електроенергії, газу, води, тепла, а також володіти додатковими можливостями, які розглядаються нижче.

«Розумний» прилад обліку володіє наступними технічними особливостями:

1. Формує і зберігає поточні і архівні значення спожитих енергоресурсів. Обсяг архівних даних залежить від розміру пам'яті контролера приладу.

2. Має вбудований годинник реального часу, які вимагають періодичної синхронізації з єдиного центру.

3. Володіє можливістю взаємодії з інформаційною системою, що управляє для формування балансу споживання, обліку допуску приладу.

4. Має стандартний цифровий інтерфейс для обміну даними з автоматизованою системою обліку споживання енергоресурсів та (або) телекомунікаційну частину для віддаленої передачі даних в центр обліку та розрахунків.

Основні вимоги, що пред'являються до «розумних» мереж, такі:

- можливість «самовідновлення» мережі після замикань, фізичних ушкоджень та ін.;
- можливість мотивування споживачів для активної участі в регулюванні мережі (за допомогою регулювання власного споживання);
- висока стійкість до шкідливих зовнішніх впливів (теракти, диверсії і т.п.);
- можливість надання електроенергії високої якості (в т.ч. з заданими параметрами) і скорочення втрат;
- інтеграція опцій виробництва і зберігання електроенергії; висока ефективність.

Розвиток технологій «розумних» мереж (Smart Grid) і «розумних» лічильників (Smart Metering) несе в собі перспективу того, що всі промислові і побутові енергоприємники знайдуть здатність до взаємодії в інформаційній мережі, стануть керованими і будуть виконувати функції вимірювання власного споживання електроенергії і потужності. Це дасть реальний інструмент для енергозбереження та підвищення енергоефективності[25].

2.2.5. Розумний транспорт

Інтелектуальні транспортні системи ITS (Intelligent Transportation System) на базі технологій IoT дозволяють здійснювати автоматичну взаємодію між об'єктами інфраструктури і транспортним засобом V2I (Vehicle to Infrastructure) або між різними транспортними засобами V2V (Vehicle to Vehicle). Системи V2V здійснюють обмін даними по бездротовому зв'язку між машинами на відстані до декількох сот метрів. Системи V2I здійснюють обмін між транспортним засобом і центрами управління дорожнім рухом, операторами доріг і сервісними компаніями.

Дані, передані об'єктами інфраструктури, інтегруються в загальну систему і передаються довколишніх транспортним засобам. Технології обох груп здатні значно збільшити безпеку і ефективність транспорту.

Як приклад використання технологій IoT в містах можна привести систему управління автомобільним трафіком, яка на основі аналізу пропускної здатності доріг не тільки самостійно управляє трафіком за допомогою перенастроювання світлофорів, а й постійно в реальному часі публікує дані про свій стан, які можуть бути доступні будь-яким іншим пристроям і сервісів, будь-то ГЛОНАСС / GPS-навігатор, мобільний телефон або спеціалізовані веб-сайти. Використання технології IoT в транспортній сфері дозволяє не тільки відслідковувати оповіщення про критичні ситуації, але також перенаправляти маршрути руху в режимі реального часу і навіть попереджати пасажирів і водіїв про альтернативні маршрути, транспортних засобах, придорожньому життю і пунктах громадського харчування. Крім того, за допомогою встановлених на вулицях датчиків можна буде забезпечити публікацію інформації про їх завантаженості[26].

Серед таких «розумних» транспортних систем IoT можна згадати:

- системи запобігання зіткнень;
- системи «бічної підтримки», що вказують водію на перетин дорожніх смуг або небезпечні маневри;
- системи нічного виглядіння;
- системи автоматичного управління машиною і руху в групах машин; системи, які контролюють стан водія (зокрема, що не дозволяють йому заснути);
- системи превентивного реагування на аварійну ситуацію (наприклад, системи, що здійснюють попереднє натягування ременів безпеки перед неминучим зіткненням).

Система інформування водіїв за допомогою вбудованих в машини пристроїв VICS (Vehicle Information and Communication System) збирає інформацію через сенсори, встановлені на об'єктах дорожньої інфраструктури (дорожньому полотні, камерах спостереження та ін.), з використанням «машин-зондів» (мобільних пунктів спостереження за дорожнім рухом), а також шляхом використання вже встановлених бортових систем, що дозволяють збирати інформацію про швидкість руху транспортного потоку, погоди і стан доріг. Ця інформація системою VICS обробляється і переводиться в цифровий вигляд, а потім розсилається по бортовим навігаційним системам. Користувачі системи можуть отримувати інформацію в різних видах - у вигляді тексту, простий графіки, карт. Бортові системи динамічно обробляють дані і пропонують водієві оптимальний маршрут[27].

2.2.6. Розумне виробництво

Вважається, що винахід парової машини в XVIII столітті викликало першу індустріальну революцію. Наступний якісний стрибок стався в промисловості на початку XX століття при переході на конвеєрне виробництво. Потім, з 1960-х років, процеси на підприємствах почали кардинально змінюватися завдяки впровадженню комп'ютерів. І ось зараз ми стаємо свідками стрімко наростаючої четвертої індустріальної революції, рушійною силою якої є Інтернет речей. За рахунок технологій IoT виробничі компанії зможуть оптимізувати все - від роботи складу до виконання безпосередньо виробничих завдань, якщо кожне промислове будівництво, транспортний засіб і навіть інструмент будуть забезпечені сенсорами і регулярно будуть відправляти звіт про свій стан, місцезнаходження та інші характеристики.

Наведемо конкретний приклад. Оскільки вимоги до якості і безпеки автомобілів неухильно ростуть, виробники зацікавлені в можливості контролювати роботу основних систем і деталей вже випущених і проданих машин. Іншими словами, автозавод хоче залишатися з ними в контакті, і завдяки Всесвітній мережі це можливо. В майбутньому будь-який автомобіль стане частиною Інтернету речей. Машина зможе зв'язуватися зі своїм виробником і, наприклад, повідомляти йому, що потребує дострокове техобслуговування. Сенсори в режимі онлайн будуть сповіщати, наприклад, про перегрів, вібрації, передчасному зносі певного вузла або, скажімо, про незвичних звуках[28].

Подібні інтелектуальні цифрові системи надалі встановлюватимуть на будь-яких машинах і верстатах, але перш за все на обладнанні таких системоутворюючих об'єктів, як, наприклад, електростанції. Кожен вузол верстата або обладнання буде займатися самодіагностикою і через інтернет повідомляти про свій стан до відповідного експлуатаційний центр управління.

Такі рішення будуть мати цілий ряд переваг для самих виробників. Так, компанії зможуть краще планувати випуск і поставку запчастин, вони отримають можливість відстежувати, наскільки часто ті чи інші вузли стикаються з певними проблемами, і своєчасно вносити необхідні інженерно-конструкторські зміни. До того ж вони зможуть цілеспрямовано інформувати клієнта про необхідність замінити той чи інший вузол.

Нарешті, виробники зможуть перевіряти, чи використовує клієнт якісні фірмові запчастини або вдається до дешевих підробок. Проблема ця досить гостро стоїть сьогодні перед багатьма компаніями і в цілому машинобудівної галуззю, яка зіткнулася з потоком контрафактної продукції. Для перевірки справжності запчастин в обладнанні мешканці великої рогатої худоби. Крім стеження за будуть, наприклад, вбудовувати чіпи, які знають, де в інтернеті знаходиться відповідна документація виробника. При заміні деталей вони

перевірятимуть «Новачків» і звіряти отриману інформацію з рідною базою даних. Таким чином, машинобудівна продукція надалі буде існувати як би в двох іпостасях. Одна - реальна, «залізна», а інша - віртуальна, у вигляді набору цифрових даних.

Завдяки IoT стане можливим об'єднання всіх контрольно-вимірювальних приладів і датчиків на будь-якому виробництві в єдину інформаційну мережу. Крім ефективного витрачання енергії можна буде навіть швидко інтегрувати в систему альтернативні джерела екологічно чистої електрики - наприклад, сонячні батареї і вітряні генератори. Зниження виробничих витрат, ефективний витрата енергії, відмова від економічно нерентабельних активів - все це разом дозволить суттєво здешевити виробництво, а використання поновлюваних джерел електрики поліпшить екологічну обстановку[29].

Ще один сучасний прояв Інтернету речей - зв'язок між машинами (M2M) за допомогою SMS. В Європі цю технологію вже використовують в сільському господарстві для стеження в реальному часі за переміщенням великої рогатої худоби. Крім стеження за переміщенням худоби, фермери отримують автоматичні повідомлення про стан тварин. В стійлах і в поле встановлюються забезпечені SIM-картами пристрої для зв'язку M2M, а до тварин прикріплюються спеціальні датчики, що збирають інформацію і передають її на пристрій збору даних. Це пристрій негайно відправляє фермеру потрібну інформацію за допомогою SMS. За даними про стан тварин можна спостерігати не тільки через SMS, але і в онлайн-режимі через канал GPRS, що зв'язує системи моніторингу з центром обробки даних. У Європі таким додатком вже користуються близько 4 тисяч ферм[30].

2.2.7. Розумна медицина

«Розумна медицина» на базі Інтернету речей на практиці зазвичай реалізується у вигляді систем моніторингу здоров'я людей з використанням різноманітних біосенсорів і датчиків і систем віддаленої медичної допомоги. Можливі застосування систем моніторингу на базі сенсорних мереж в медицині:

1. Моніторинг фізіологічного стану людини: фізіологічні дані, зібрані сенсорними мережами можуть зберігатися протягом тривалого періоду часу і можуть використовуватися для медичного дослідження. Встановлені вузли мережі можуть також відстежувати рухи літніх людей, інвалідів та, наприклад, попереджати падіння. Ці вузли невеликі і забезпечують пацієнтові велику свободу пересування, в той же час дозволяють лікарям виявити симптоми хвороби заздалегідь. Крім того, вони сприяють забезпеченню більш комфортного життя для пацієнтів в порівнянні з лікуванням в лікарні.

2. Моніторинг лікарів і пацієнтів в лікарні: кожен пацієнт має невеликий і легкий вузол мережі. Кожен вузол має свою конкретну задачу. Наприклад, один може стежити за серцевим ритмом, в той час як інший знімає показання кров'яного тиску. Лікарі можуть також мати такий вузол, він дозволить іншим лікарям знайти їх в лікарні.

3. Моніторинг медикаментів у лікарнях: сенсорні вузли можуть бути приєднані до ліків, тоді шанси видачі неправильного ліки, можуть бути зведені до мінімуму. Так, пацієнти матимуть вузли, які визначають їх алергію і необхідні ліки. Комп'ютеризовані системи показали, що вони можуть допомогти звести до мінімуму побічні ефекти від помилкової видачі препаратів[31].

Одним з етапів вдосконалення сучасної медицини є персоналізація даних і підвищення комунікації між лікарями. Легкий доступ до історії

хвороби, дозволяє призначати своєчасне ефективне лікування. Ведення медичних карт поступово може перейти в мережу. «Хмарні» рішення використовуються для зберігання великих обсягів інформації в інтернеті. Завдяки інтернету лікарі різних клінік отримують доступ до даних пацієнта. Електронні медичні картки дають змогу вчасно дізнаватися про здоров'я хворого, призначати ефективне лікування. Зв'язування обладнання медичного закладу в єдину мережу дозволить отримувати необхідні дані на портативні пристрої лікарів, на які надходить інформація про пацієнта: які ліки прописані, результати аналізів і т.д.

Впровадження інтернет-технологій заощаджує час пацієнта і лікаря. Не треба добиратися до поліклініки, варто тільки включити комп'ютер і можна зв'язатися з медичним закладом. Відео виклик дають можливість не тільки провести опитування, а й зробити загальний огляд, що часто досить для загального уявлення про здоров'я людини. Якщо все-таки необхідна зустріч з лікарем, то записатися на прийом можна також через інтернет.

Апарати для вимірювання тиску, ваги та інше портативний обладнання оснащується бездротовими передавачами, які дозволяють дані відразу переносити на комп'ютер і вести облік за своїм здоров'ям. Розробивається «розумна одяг», яка збирає дані про стан людини: частоту серцевого ритму, температуру тіла, частоту дихання. У таку розумну одяг вшиваються ще на стадії розробки чіпи, які не тільки проводять вимірювання, але і дозволяють передавати дані на мобільний телефон[32].

2.2.8. Розумне життя

Вже важко когось здивувати доставкою продуктів на будинок, але компанія Electrolux вирішила зробити крок ще далі, представивши свою нову розробку - робота АММІ, що ходить за покупками замість свого власника. АММІ - це, по суті, корзина для покупок, которая доставить продукти на будинок, при цьому зберігаючи їх свіжість за допомогою термоелектричного

охолодження. Господарю робота потрібно тільки зробити он-лайн замовлення в магазині і потім відправити робота, щоб він його забрав. АММІ оснастили GPS- навігатором, для того, щоб він міг легко знайти дорогу до супермаркета, а також гіроскопом для безпеки перемещення вулицями міста і системою безпілотного руху.

Комп'ютеризована взуття Verb for Shoe («Команда для взуття») компанії VectraSense має вбудований спеціалізований мікрокомп'ютер ThinkShoe (з ультранизьким витратою енергії), що працює під управлінням спеціальної операційної системи Magellan і здатний поступово навчатися[33].

Висновки:

Для реалізації IoT необхідна екосистема, яка включала б у себе «розумні речі» – різні пристрої, оснащені датчиками; мережу доступу і передачі інформації, а також платформи для управління мережею, пристроями і додатками. Для передачі даних від «розумних» пристроїв сьогодні існує чимало спеціалізованих стандартів та протоколів.

У цьому розділі розглядаються основні протоколи та стандарти для взаємодії між пристроями IoT, без яких майже неможливо уявити собі правильну і ефективну роботу Інтернету речей. Стандарти необхідні для двостороннього обміну інформацією та інформацією між речами, їх навколишнім середовищем і організаціями, які зацікавлені в моніторингу та контролі.

Також розглядаються такі програмно-апаратні рішення, як: «Розумна планета», «Розумне місто», «Розумний будинок», «Розумна енергія», «Розумний транспорт», «Розумне виробництво», «Розумна медицина» та «Розумне життя». Було оглянуто особливості керування даними в таких рішеннях.

РОЗДІЛ 3.

АНАЛІЗ ПРОБЛЕМ УПРАВЛІННЯ ПОТОКАМИ ДАНИХ В ІОТ

Одна з основних проблем розвитку IoT – ефективно та розумно керувати даними. Управління даними IoT включає в себе процес збору, обробки, зберігання та аналізу даних. Першою та основною метою є збір точних і достовірних даних з багатьох джерел та управління неоднорідними структурами даних. По-друге, для підтримки прийняття рішень необхідно витягувати високорівневу інформацію та робити висновки з вихідних даних. Врешті-решт, як зберігати та аналізувати велику кількість даних, також є ключовою проблемою для IoT програм.

3.1 Загальні характеристики даних IoT

У загальному випадку дані Інтернету речей мають чотири різні характеристики:

- *Гетерогенність.* IoT використовує різні властивості в різних типах даних для опису стану "речей". Ці типи даних варіюються від цілого числа до символу, включаючи напівструктуровані та неструктуровані дані, такі як аудіо- та відеопотоки.
- *Неточність.* Одним з основних факторів, що обмежує широке поширення Інтернету речей, є неточність отриманих даних. Наприклад, експерименти показують, що RFID-системи можуть захоплювати лише 60-70% правильних даних, викликаних ненадійними показаннями, що призводить до труднощів для прямого використання. Така ж ситуація спостерігається і в більшості інших технологій зондування.
- *Масивні дані в режимі реального часу.* IoT призначений для з'єднання тисяч об'єктів у великих масштабах. Зв'язок між різними об'єктами в

динамічних мережах генерує великий об'єм неоднорідних даних у формі реального часу, швидкісних, безперебійних потоків даних. Масштабні схеми зберігання, фільтрації та стиснення важливі для ефективної обробки великих даних.

- *Неявна семантика.* Необроблені дані IoT мають низький рівень зі слабкою семантикою. Для підтримки додатків вищого рівня, таких як «розумний дім» та «розумна медицина», складну семантику потрібно абстрагувати з маси даних низького рівня[34].

3.2 Еталонна модель управління даними IoT

Відповідно до перелічених вище характеристик, розглянемо еталонну модель управління даними IoT (Рисунок 3.1). Модель складається з трьох рівнів:

- 1) Рівень очищення даних.

Оскільки надійність сучасних систем Інтернету речей далека від практичного використання, очищення даних необхідно для правильної інтерпретації та аналізу даних Інтернету речей. Основна мета цього рівня - зменшення ненадійності даних. Враховуючи величезний обсяг інформації, гетерогенні джерела помилок і вимоги до обробки даних в реальному часі, це може бути складним завданням[35].

- 2) Рівень обробки подій.

Очищені дані IoT відрізняються високою надійністю та зручністю використання. Але необроблені дані надають лише просту інформацію, яка безпосередньо не пов'язана з бізнес-процесами. Рівень обробки подій робить висновки і перетворює необроблені дані в бізнес-логіку вищого рівня. Для цього застосовується семантична методика[36].

3) Рівень зберігання та аналізу даних.

Маючи дані у формі бізнес логіки, системи IoT повинні надавати послуги в різних аспектах і зберігати їх за відповідною схемою. Така схема повинна стискати кількість даних та підтримувати аналіз у різних ієрархіях.

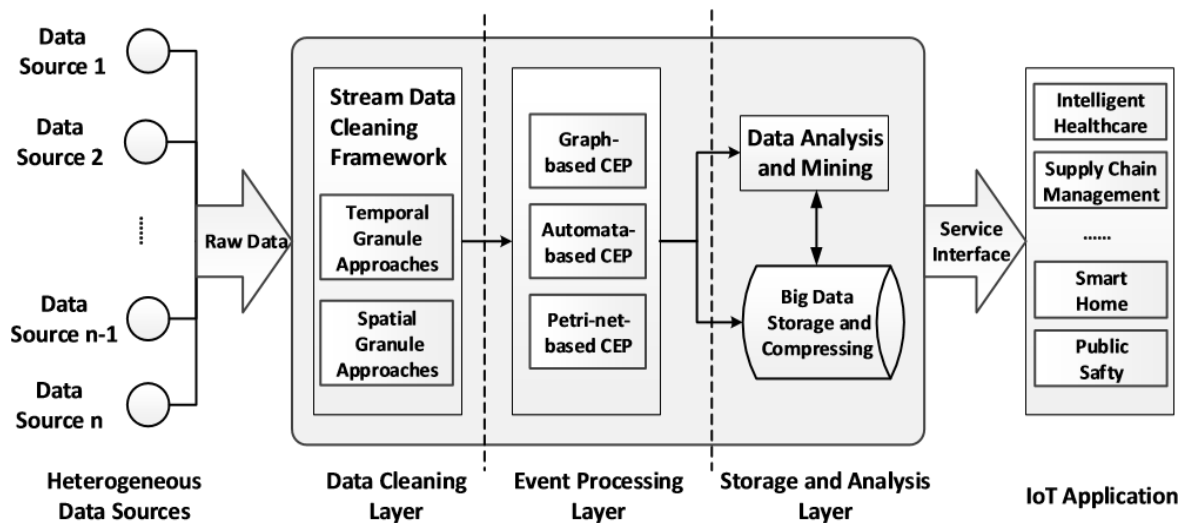


Рис. 3.1 Еталонна модель управління даними IoT.

3.3 Проблеми управління даними IoT та підходи до їх вирішення

У цьому розділі розглянемо типові проблеми, що виникають на кожному рівні, та відповідні підходи, щодо вирішення цих проблем.

Рівень очищення даних:

Поняття очищення даних вперше було введено в дослідженні сховищ даних, яке має на меті очищення неповних, помилкових та повторюваних даних, щоб нарешті вирішити питання якості даних у базах даних чи файлових системах. Однак, на відміну від баз даних або файлових систем, ненадійність даних, що виробляються датчиками IoT, а саме так званих "брудних даних", проявляється у чотирьох загальних формах: *хибнонегативні, хибнопозитивні, недійсні та надлишкові*. Хибнонегативні

відносяться до втрати даних у датчиках IoT. Причиною цієї проблеми є перешкоди між датчиками та складним середовищем. Хибнопозитивні дані також відомі як шум. Окрім правильних даних, система також може збирати додатковий шум, який не передбачений. Це також обумовлено чинниками самого датчика та середовищем зв'язку. Також це спричинить ще одну проблему під назвою недійсні дані, які показують, значення, що відхиляється від нормального діапазону. Для забезпечення покриття сигналу, як правило, більше одного датчика охоплює один і той же об'єкт. Така політика спричиняє надлишковість даних. Технологія очищення даних в IoT широко вивчена. Підходи до зменшення та усунення проблем якості даних включають в себе системи очищення потокових даних та підходи часових і просторових гранул[37].

1) Система очищення потокових даних

Система очищення даних – це організаційна структура підходів до очищення даних у різних рівнях обробки та точках зору. Гнучка лінійна структура очищення даних сенсорів, названа ESP (Extensible Sensor stream Processing) описується в багатьох наукових роботах. ESP складається з п'яти етапів: *Виділення, Згладжування, Об'єднання, Арбітражу та Віртуалізації*. Етап виділення виділяє єдине значення даних як окреме. Етапи згладжування та об'єднання призначені для обробки даних відповідно у часових та просторових гранулах. Логічні помилки усуваються на стадії арбітражу, а дані з багатьох джерел поєднуються на етапі віртуалізації. Ця система забезпечує ефективну та гнучку організацію обробки даних. Проте, питання, як вибрати конкретну часову та просторову гранули для різних сценаріїв застосування, залишається невирішеним. Оскільки вартість алгоритму та ефективність різних підходів до очищення не враховані в ESP, представлена система очищення з мінімізацією обчислювальних витрат. Ця система, орієнтована на витрати, базується на ідеї класифікатора, який визначає вартість очищення/помилки для RFID і результатом її роботи є дерево

рішень з мінімальними витратами на очищення тестів машинного навчання. Хоча ці системи очищення даних для IoT можуть ефективно організовувати різні алгоритми з різних аспектів, вони засновані на послідовній комбінації алгоритмів. Структурування та оптимізація підходів до майнінгу даних можуть бути впроваджені в дослідження систем для підвищення ефективності[38].

2) Підхід часових гранул

Підхід часових гранул до очищення даних в основному базується на концепції згладжування часових вікон. Як показано на рисунку 3.2, ідея алгоритму полягає у виведенні показань в кінці часового проміжку, якщо в цьому вікні є принаймні одне позитивне значення.

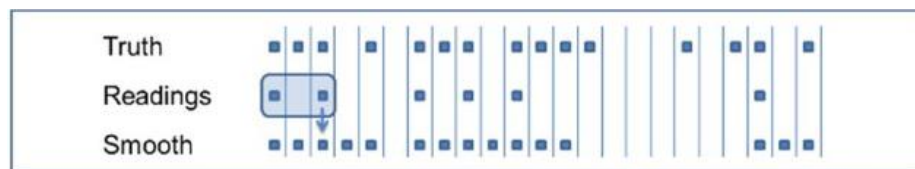


Рис. 3.2. Згладжування вікон фіксованого розміру

Хоча згладжування вікон фіксованого розміру є ефективним та простим у виконанні, воно не може забезпечити одночасно повноту та динаміку даних. Для вирішення цієї проблеми SMURF вводить адаптивну віконну схему, розглядаючи потоки даних як статистичний зразок показань. Багато вдосконалень SMURF представлені в очищенні показань об'єктів, які швидко рухаються, високоточне визначення ваги вузлів та статистичного очищення на основі датчиків відстані. Підходи часових гранул можуть бути відображені на стадії згладжування в рамках системи ESP. Ця система може очищати дані на основі їх статистичних характеристик. Хоча SMURF та його алгоритми вдосконалення досягають хорошого балансу між повнотою та динамікою, підхід часових гранул є низькорівневим механізмом очищення. Очищення даних більш високого рівня вимагає додаткової просторової та логічної інформації для досягнення кращих результатів[39].

3) Підхід просторових гранул

Підхід просторових гранул може бути реалізований у етапі об'єднання в рамках системи ESP. Основна його мета - очищення та агрегація даних з різних джерел. Розподілена архітектура системи RFID, заснована на зв'язку між зчитувачами по захищеному каналу. Аналогічно, як показано на рисунку 3.3 розгортання системи IoT можна розділити на зони. Міжзональні комунікації можуть надавати важливу інформацію та підтримку очищення даних підходом просторових гранул.

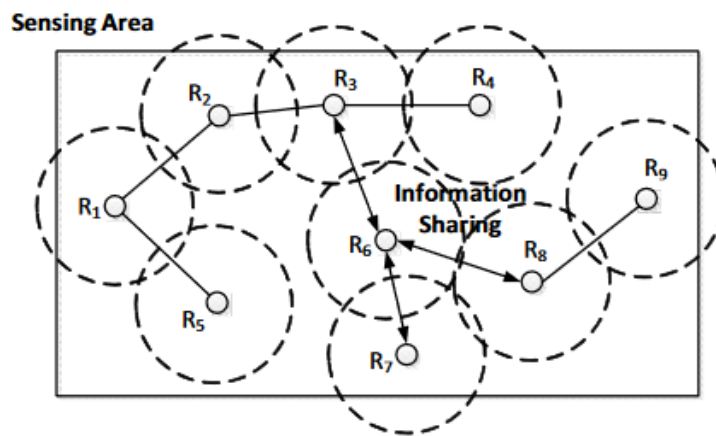


Рис. 3.3 Розподілена модель на основі міжзональної комунікації

Співпраця P2P - це метод очищення даних RFID, що діє аналогічно мережі P2P, заснований на архітектурі міжзональних комунікацій. Завдяки обміну інформацією з наступними і подальшими вузлами, чутливий вузол може визначити і виправити помилку за допомогою сусідніх вузлів. Аналогічно, TopK-PDI та bSpace видаляють повторювані та хибнопозитивні дані, використовуючи обмін даними між зчитувачами RFID. На жаль, ця архітектура має більш високі вимоги до можливостей комунікації між пристроями та контролю топологією системи[40].

4) Підсумок

У Таблиці 3.1 узагальнено основні підходи до очищення даних IoT та їх характеристики.

Таблиця 3.1

Класифікація підходів до очищення даних IoT

	Ціль	Гранула	Етап ESP	Особливості
ESP	ХН, ХП, Не, На	Ч, П	Ви, З, О, А, Ві	Цілісна система
Орієнтована на витрати	ХН, ХП	Ч	Ви, З, О	Мінімальна вартість очищення
Вікна фіксованого розміру	ХН, ХП	Ч	Ви, З	Проста та ефективна
SMURF	ХН, ХП	Ч	Ви, З	Баланс повноти та динаміки
P2P співробітництво	ХН, ХП	Ч, П	Ви, З, О	Подібна до P2P система очищення
TopK-PDI	ХП, На	Ч, П	Ви, З, О	Міжзональна комунікація
bSpace	ХН, ХП	Ч, П	Ви, З, О	Байєсівська оцінка

Примітка: ХН - Хибнонегативний, ХП - Хибнопозитивний, Не - Недійсний, На - Надлишковий, Ч - Часова, П - Просторова, Ви - Виділення, З - Згладжування, О - Об'єднання, А - Арбітраж, Ві – Віртуалізація.

Виходячи з вищенаведеного аналізу, можна сказати, що існуючі алгоритми та системи в більшості випадків розроблені для систем RFID. Розширення цих досліджень від RFID до систем IoT матиме широкі можливості для дослідження управління даними IoT.

Рівень обробки подій:

Подія – це явище інтересу в певний час, який може бути або примітивною, або складною подією. В системах IoT очищені дані можуть трактуватися як примітивні події. Як показано на рисунку 3.4, на рівні обробки подій складні семантичні події витягуються з примітивних подій низького рівня для підтримки додатків більш високого рівня, що називається комплексною обробкою подій (CEP). CEP розгортається для виявлення зацікавлених моделей поведінки та виконання таких задач, як виявлення подій, їх моніторинг та реагування на них[41].

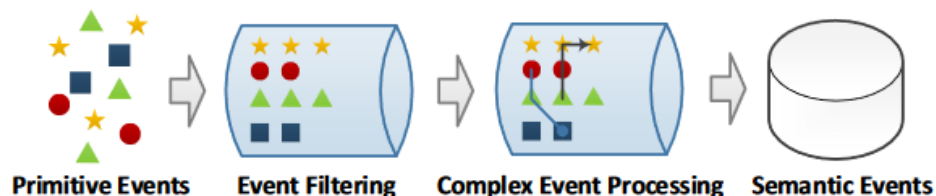


Рис. 3.4 Комплексна обробка подій в IoT

Згідно з нашим дослідженням, існуючі моделі CEP можна класифікувати на три категорії:

1) Модель CEP на основі графіків

У моделі на основі графіків складні події виражаються в структурі дерева, а його листя-вузли представляють примітивні події. Після того, як відповідна подія відбудеться, випадок буде зберігатися у вузлі та переміщений до його батьківського вузла. Якщо батьківський вузол успішно виявить відповідність до семантики його операцій, результат буде надалі переміщений у верхній вузол, поки корінь не виявить, що ця складна подія відбудеться. Snoor є першою системою CEP, яка забезпечує просту підтримку графічної моделі часу для виявлення складних подій в активній системі баз даних. READY та YEAST – це інші системи CEP, засновані на графічній моделі. Основним недоліком цих підходів є відсутність поглибленої підтримки обмежень складних часових подій. RCEDA надає детальну мову опису часових обмежень у складній події та пропонує

концепцію неспонтанної події. Багато подій не є спонтанними, оскільки вони не можуть виявити їх випадки самостійно, поки не закінчився термін дії, якщо вони пов'язані з інтервальними обмеженнями. RCEDA визначає ЕСА-подібну мову опису для вираження складних подій та використовує псевдо-подію для неспонтанної обробки подій[42].

2) Модель CEP на основі механізмів

У цій моделі подія будується у відповідні механізми, набір станів та перехідних функцій в автоматизованій моделі. Складна подія успішно виявляється, якщо механізми досягають стану прийняття відповідно до історії подій. У базі даних Ode спочатку приймаються механізми з кінцевим станом для виявлення складної події, яка описується мовою, заснованою на логіці. Cauuga та Esper використовують механізм автоматизації для обробки подій з потоків даних. Однак неспонтанна подія не підтримується цими підходами. SASE – це механізм CEP, заснований на механізмах, що підтримує неспонтанне виявлення подій. Він забезпечує структуру запитів на основі плану для обробки події, яка включає п'ять етапів: послідовність сканування/побудова, вибір, вікно, заперечення та трансформація[43].

3) Модель CEP на основі петрі-мережі

У цій моделі комплексна подія трансформується у відповідну мережу петрі в моделі CEP на основі петрі-мережі. Місце введення інформації представляє примітивну подію, а місце виводу вказує на виникнення складної події. Місце введення буде позначено, коли відбудеться відповідна подія. Якщо всі місця введення позначені, перехід буде запущено. Складна подія успішно виявляється, коли модель досягає місця виходу. Модель на основі мережі петрі вперше була використана SAMOS у активному виявленні подій у базі даних. В проміжному програмне забезпечення CEP, представлено систему PRES, яка надає низку тимчасових конструкторів для опису та обробки неспонтанних подій[44].

У таблиці 3.2 узагальнено основні моделі обробки подій IoT та їх характеристики.

Таблиця 3.2

Класифікація підходів до обробки подій в IoT

	Модель	Мова	Логічний конструктор	Часовий конструктор	Пасивні події
Snoop	Графічна	Правила ECA	or, and тощо	Є	Не підтримуються
YEAST	Графічна	Мова специфікації YEAST	Базова логіка	Нема	Не підтримуються
RCEDA	Графічна	Правила подібні до ECA	Λ, V тощо	Є	Підтримуються
Cayuga	Механізми	Мова подій Cayuga	Базова логіка	Нема	Не підтримуються
SASE	Механізми	Мова подій SASE	Базова логіка	Є	Підтримуються
Esper	Механізми	EPL	та, або, не тощо	Є	Не підтримуються
SAMOS	Мережа петрі	Правила ECA	Базова логіка	Нема	Не підтримуються
PRES	Мережа петрі	Мова подій PRES	&, тощо	Є	Підтримуються

Великий обсяг даних з різномірних джерел зі складним семантичним значенням є великим викликом для обробки подій в IoT, а відсутність смислової підтримки в обробці ускладнює реальні застосування. Точне семантичне визначення та обробка інформації, однак, може досягти широкого спектру несумісності між інформаційними системами. Тим часом,

семантична підтримка все ще відсутня частина існуючих рішень. Онтологія, яка є формальною специфікацією спільної концептуалізації, може бути важливим інструментом побудови концепції та взаємозв'язку між "речами" в IoT. Ми вважаємо, що семантична обробка подій IoT на основі онтології є перспективною темою дослідження.

Рівень зберігання та аналізу даних:

Обмін, зберігання та стиснення даних для IoT реалізовані на рівні зберігання та аналізу даних. Як керувати неоднорідними масивними даними IoT в реальному часі – це складна і ключова тема дослідження.

1) Мова обміну інформацією

Дані повинні передаватись між різними пристроями IoT, регіонами та системами. Через наявність неоднорідної платформи нам потрібна міжплатформна мова для обміну інформацією для ефективної комунікації. XML застосовується для обміну інформацією в Інтернеті у багатьох системах. Як результат, багато мов обміну інформацією IoT розроблені на основі XML. PML (Physical Markup Language) – один із стандартів обміну інформацією IoT, розроблений EPCGlobal для опису зв'язку між фізичними середовищами та об'єктами. Підтримувані програми включають відстеження інвентарю, автоматичні транзакції, управління ланцюгами поставок та комунікацію між об'єктами. IEEE 1451 – ще один важливий стандарт інтерфейсу для розумних сенсорів та датчиків. SensorML запропонований OGC (Open GIS Consortium), що забезпечує стандартні моделі та кодування XML для опису датчиків та процесів вимірювань на основі IEEE 1451. Інші стандарти, включаючи TML, EXDL, M2MXML та BITX, зведені в таблиці 3.3[45].

Таблиця 3.3

Класифікація мов обміну інформацією IoT

	Стандарт	Галузь	Вміст
PML	XML	Логістика, транспорт, охорона здоров'я, виробництво	Дані системи EPC
SensorML	IEEE 1451	Додатки датчиків	Передача даних сенсору
TML	XML	Екологічна, медична, промислова сфери, сфера безпеки тощо.	Обмін даними між сенсором та додатком
EXDL	XML	Медицина, Розумне Місто	Екстрені повідомлення
M2MXML	XML	Розумне управління пристроями	Обмін даними між розумними пристроями
BITXmI	XML	Розумне управління пристроями	Управління та зв'язок між розумними пристроями

Ці мови зосереджені на різних областях застосування, що ускладнює обмін інформацією між системами IoT. Семантичний пошук та обробка перехресних галузей також важка в реалізації, оскільки вони не мають однакової базової концепції онтології. Тому визначення єдиної концепції онтології та мови обміну інформацією, що охоплює різні сфери застосування, є важливою роботою у майбутньому.

2) Стиснення та зберігання даних

Великий обсяг даних є головним проблемою управління даними в IoT. У багатьох наукових дослідженнях запропоновано кілька рішень для стиснення даних у сховищах. Структура даних у вигляді бітових карт пропонується для того, щоб компактно представляти набір даних EPC. Цей тип даних використовує ключове спостереження, що він є більш ефективним у відстеженні згрупованих даних EPC, ніж коли дані відстежуються окремо. Це легко реалізувати в СУБД, і визначено ряд операцій для оперативного перетворення, обслуговування та обчислення. Крім даних EPC, запропонована ефективна схема кодування шляху, що використовується для кодування інформації про потік для моніторингу логістичних продуктів. Ця схема кодування заснована на *Китайській Теоремі Залишків* та *Унікальній Теоремі Факторизації*. Інформація про час кодується в структуру дерева, подібну до кодування області XML. Ця схема може ефективно отримувати запити щодо трекінгу та шляху. Концепція сховища даних RFID для онлайн аналітичної обробки під назвою RFID-Cuboids розроблена на основі спостереження, що об'єкти RFID зазвичай рухаються великими групами, а аналіз даних проводиться на різних рівнях абстракції. Схема зіркового зберігання побудована на основі таблиці фактів з назвою Stay і пов'язана з іншими підтримуючими таблицями. Хоча аналіз RFID-кубоїдів підтримується лише тимчасовим та просторовим виміром розміру, як показано на рисунку 3.5, ми можемо розширити додаткові типи даних, що робить аналіз можливим в інших вимірах. Вищезгадана схема стиснення та зберігання створена виходячи з припущення, що об'єкти сканування переміщуються в групі, так що дані мають велику схожість. Якщо це не так, ефективність використання цих схем зберігання даних буде відносно низькою[46].

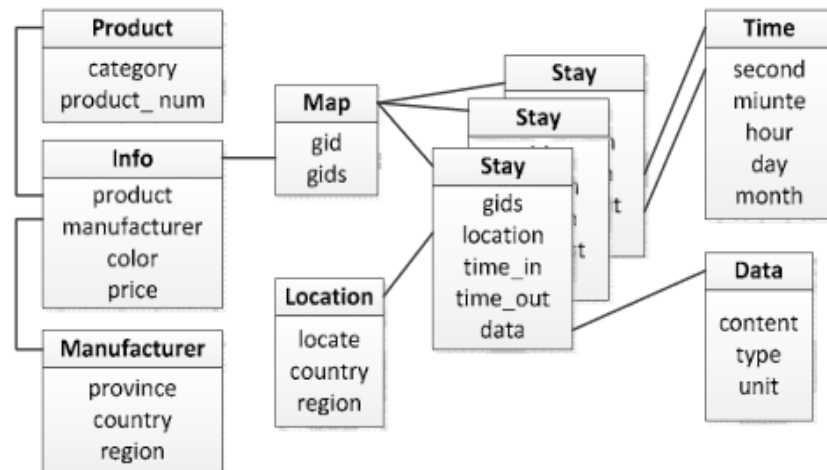


Рис. 3.5 Розширена схема зберігання для RFID-кубоїдів

3) Зберігання та обробка великих даних

Принципова мета IoT полягає у розумному реагуванні та прийнятті рішень у доменних додатках на основі точного сприйняття та розумної обробки даних. IoT також є одним із типових нових доменів, у яких дані накопичуються з високою швидкістю та кількістю. Як гаряча тема для досліджень, обробка великих даних є однією з важливих частин управління даними в IoT. Великі дані – це великий і складний набір даних або потік даних, який важко обробити, використовуючи традиційні засоби управління базами даних або програми обробки. Швидкий розвиток сенсорних технологій робить управління даними IoT складнішим, особливо для великої кількості неструктурованих даних. У таблиці 3.4 узагальнено та порівняно характеристики великих даних в IoT з іншими областями їх застосування[47].

Таблиця 3.4

Типові сфери обробки великих даних

Сфера	Приклади застосування	Масштаб використання	Швидкість даних	Масштаб даних	Тип даних
Інтернет речей	Дані сенсорів	Великий	Швидкі	ТВ	Складні

Продовження таблиці 3.4

Сфера	Приклади застосування	Масштаб використання	Швидкість даних	Масштаб даних	Тип даних
Наукові розрахунки	Біометрика	Маленький	Повільні	TB	Прості
Фінансова аналітика	Транзакції	Великий	Швидкі	GB	Прості
Соціальні мережі	Web2.0	Дуже великий	Швидкі	PB	Складні
Мобільні мережі	Смартфони	Дуже великий	Швидкі	TB	Складні
Мультимедіа	Аудіо, Відео	Дуже великий	Швидкі	PB	Прості

Існує дві обчислювальні парадигми для обробки великих даних в IoT: *Потік Даних* та *MapReduce*. У моделі потоку даних дані надходять у якості потоку, а алгоритм обробки покладається на дані без явного їх зберігання. Очищення даних часових гранул та обробка подій часового вікна – це підходи до обробки даних, засновані на моделі потоку даних. Типові системи обробки великого потоку даних у реальному часі, які можуть полегшити процес, включають Twitter Storm, Yahoo S4 та LinkedIn Kafka. У моделі MapReduce дані розподіляються в підлеглих машинах, а обчислення виконуються в послідовності карти і скорочення операцій. Хмарні обчислення стали стандартною платформою для аналізу великих даних. Існує багато споріднених досліджень щодо зберігання даних, розподіленої обробки даних та обміну даними на платформі хмарних обчислень[48].

Проміжне програмне забезпечення для управління даними в IoT

Проміжне програмне забезпечення – це тип програмного забезпечення, яке надає послуги додаткам, дозволяючи комунікації та управління даними в розподілених системах, таких як IoT. У звіті, опублікованому ISO/IEC,

функції проміжного програмного забезпечення для сенсорних мереж включають збір інформації, фільтрування, аналіз, прийняття рішень і т.д. Системи проміжного програмного забезпечення для управління даними в IoT зазвичай підпадають під такі категорії:

1) Модель на основі віртуальної машини

Модель на основі віртуальної машини складається з віртуальних машин (VM) та інтерпретатора скриптів. Зазвичай вони надають набір інструкторів програмування мовою, подібною до асемблеру. Інструктори користувача інтерпретуються та завантажуються у віртуальну машину для виконання. Типові рішення для проміжного програмного забезпечення включають Mate, SensorWare та MagnetOS. Ця модель має високу гнучкість в інтерфейсі для полегшення розробки програмістами під неоднорідне обладнання. Однак, вона має недоліки в залежності від інтерпретатора коду та високих накладних витратах на систему. Крім того, програмування на низькорівневій мові типу асемблеру, є досить важким у використанні.

2) Модель на основі бази даних

Модель на основі бази даних дозволяє простий, декларативний стиль запитів, який подається в систему і повертає результат, як у базі даних. Проміжне програмне забезпечення управляє мережею як віртуальною базою даних, а вузли – як об'єкти розподілу даних. Такі рішення, як TinyDB, Cougar та SINA, реалізовані в моделі на основі бази даних, і вони можуть забезпечити управління та оптимізацію вузлів, даних та запитів. Ця абстракція високого рівня гарантує незалежність програм для обробки даних з набором простих інтерфейсів запитів. Тим не менше, модель на основі бази даних повинна встановлювати і підтримувати загальну абстракцію розподільних вузлів і топологію системи. Це обмежує розширюваність і позбавляє поглибленого контролю над системою.

3) Модель на основі подій

Модель на основі подій – це орієнтована на повідомлення парадигма, що використовує механізм "Publish-Subscribe", що дозволяє вільний асинхронний обмін повідомленнями між відправником та одержувачем. Ця парадигма підходить для всеосяжних сценаріїв з великою кількістю подій, таких як охорона здоров'я та фінансові дані. Проміжні системи, такі як Mires, DSWare та PSWare, забезпечують комплексну побудову та виявлення подій. ALE – специфікація подій на рівні додатків для зв'язку за інтересами події між додатками та джерелами даних EPC. Є багато промислових рішень, заснованих на специфікації ALE. Хоча проміжне програмне забезпечення, що базується на подіях, має багато переваг і може бути швидко розроблене, порівняно з технологією CEP, виявлення подій у режимі реального часу, надійність обслуговування та безпека інформації в проміжному програмному забезпеченні, що базується на подіях, все ще потребують подальшого вивчення[49].

4) Модель на основі сервісів

Проміжне програмне забезпечення IoT на основі сервісів, наприклад (SI)², SensorAct та Hydra, базується на сервісно-орієнтованій архітектурі (SOA). За підтримки SOA стандартні сервіси надаються для досягнення гнучкого та масштабованого програмування та спрощення процесу розробки додатків. Ця модель є багатообіцяючою, оскільки може об'єднатись та використати переваги інших моделей, таких як моделі на основі баз даних або подій. Співпраця та інтеграція з хмарними обчисленнями, питання конфіденційності інформації та якість обслуговування (QoS) є головними проблемами для дослідження.

5) Інші моделі

Інші основні підходи проміжного програмного забезпечення IoT включають проміжне програмне забезпечення на основі самоадаптивних та мобільних агентів. MiLAN і TinyCubus – це самоадаптивні системи

проміжного програмного забезпечення, які можуть постійно адаптувати мережеву конфігурацію відповідно до зворотного зв'язку з додатків. Проміжне програмне забезпечення на основі мобільного агента може інтелектуально мігрувати та клонувати агенти до потрібних місць разом із змінами в мережі. TinyLime та Agilla – типові рішення цієї моделі[50].

б) Підсумок

У таблиці 3.5 показані основні рішення проміжного програмного забезпечення щодо їх характеристик та підтримуваних функцій, особливо семантики, безпеки та QoS. Як показано в таблиці 3.5, інтелектуальна обробка даних є першою проблемою та можливістю в дослідженнях проміжного програмного забезпечення. Крім того, проблема QoS, наприклад, як забезпечити зручність послуг та надійність часу обробки, є ще одним ключовим питанням дослідження. Також, досліджень щодо захисту даних та управління конфіденційністю все ще недостатньо.

Таблиця 3.5

Рішення проміжного програмного забезпечення щодо їх характеристик та підтримуваних функцій

Модель	Проміжне ПЗ	Платформа	Семантика	Безпека	QoS	Особливості
Віртуальна машина	Mate	TinyOS	X	X	X	Набір інструкцій та інтерпретатор
	SensorWare	ARM Platform	X	X	X	Мова скриптів на базі tcl
	MagnetOS	Java VM	X	X	X	Гнучке розгортання на основі компонентної архітектури
База даних	TinyDB	TinyOS	X	X	X	Розподілена архітектура потоку даних
	Cougar	MICA, Unix	X	X	X	Розподілена мова запитів аналогічна мовам баз даних
	SINA	Sensor Node	X	X	X	Розподілена по рівням структура кластерів вузлів
	SwissQM	Java VM	X	X	X	Поеднання SwissQM VM та мови запитів бази даних
Подія	Mires	TinyOS	--	X	X	Парадигма обміну даними "Publish-Subscribe"
	DSWare	Sensor Node	--	X	X	Введення функції довіри для усунення недостовірності одного вузла

Продовження таблиці 3.5

	Impala	ARM Platform	--	X	X	Легка система розподілу подій
	PSWare	Java VM	✓	X	X	Гнучка композиція складних подій
	ALE	EPC	--	--	--	Широка підтримка промислових виробників
Сервіс	(SI)²	SOA	--	X	X	Сервісний інтерфейс для смарт-пристроїв
	SensorAct	Java VM	✓	✓	X	RESTful API, механізми захисту конфіденційності повідомлень
	Hydra	SOA	✓	✓	✓	Комплексне середовище розробки для IoT
Інші	MiLAN	Sensor Node	X	X	✓	Самоадаптивний стек мережних протоколів
	TinyCubus	TinyOS	X	X	✓	Динамічна система та структура обробки даних
	TinyLime	TinyOS	X	X	X	Міграція агентів та клони
	Agilla	TinyOS	✓	X	X	Простір, схожий на Linda, для взаємодії між агентами та виявлення контексту

Примітка: ✓ Функція підтримується, X Функція не підтримується, -- Не визначено однозначно

Висновки:

Серед багатьох різних проблем розвитку IoT можна виділити наступну – ефективно та розумно керувати даними. Керування даними IoT включає в себе процес збору, обробки, зберігання та аналізу даних. Першою та основною метою є збір точних і достовірних даних з багатьох джерел та управління неоднорідними структурами даних. По-друге, для підтримки прийняття рішень необхідно витягувати високорівневу інформацію та робити висновки з вихідних даних. Врешті-решт, як зберігати та аналізувати велику кількість даних, також є ключовою проблемою для IoT програм.

В цьому розділі розглядаються:

- 1) Загальні характеристики керування даними.
- 2) Еталонна модель управління даними IoT.
- 3) Було висвітлено типові проблеми, що зустрічаються в кожному рівні еталонної моделі управління даними IoT.
- 4) Підходи до вирішення проблем керування даними в IoT.

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

1. Було вивчено історію виникнення Інтернету речей, представлені найбільш актуальні сфери застосування та перспективи використання IoT. Можна сказати, що IoT має великий потенціал для розвитку майже у всіх сферах. Незалежно від області застосування, метою Інтернету речей є підвищення якості повсякденного життя людей та великий вплив на економіку та суспільство.

2. Були приведені загальні проблеми розвитку ринку Інтернет речей. В роботі висвітлені такі проблеми, як: відсутність певних стандартів, нездатність датчиків працювати незалежно від змінних або вимагаючих заряду пристроїв живлення. Особливу важливість також набувають питання безпеки самої системи. Легко припустити, які можливі наслідки може спричинити за собою недостатня забезпеченість системи, відсутність в ній необхідних протоколів безпеки та шифрування даних.

3. Проведено огляд існуючої архітектури IoT. Інтернет речей складається з набору різних телекомунікаційних технологій, що забезпечують функціонування IoT. За допомогою його архітектури, яка складається з чотирьох функціональних рівнів, можна розглянути, як ці технології пов'язані одна з одною.

4. Розглянуто основні протоколи та стандарти для взаємодії між пристроями IoT. Проаналізувавши основні протоколи та стандарти IoT, можна сказати, що для «Інтернету речей» потрібно безліч протоколів. Всі стандарти та протоколи, які були розглянуті в даній роботі, помітно відрізняються між собою. Простіше за все класифікувати їх за кількома ключовими параметрами: якістю сервісу, адресацією і за додатком протоколів. Ключові особливості протоколів залежать і від їх передбачуваного застосування.

5. Проаналізовані такі програмно-апаратні рішення, як: «Розумна планета», «Розумне місто», «Розумний будинок», «Розумна енергія», «Розумний транспорт», «Розумне виробництво», «Розумна медицина» та «Розумне життя». Було розглянуто особливості керування даними в таких рішеннях.

6. Проведено аналіз загальних характеристик керування даними та розглянуто еталонну модель управління даними IoT, яка складається з трьох рівнів. Кожний з цих рівнів має свої завдання. Таким чином, метою першого рівня є зменшення ненадійності даних. Другий рівень робить висновок і перетворює необроблені дані в бізнес-логіку вищого рівня. Завданням третього рівня є зберігання та аналіз отриманих даних.

7. Було висвітлено типові проблеми, що зустрічаються в кожному рівні еталонної моделі управління даними IoT та проаналізовано підходи до вирішення проблем керування даними в IoT. Серед всіх проблем, найбільш актуальними можна виділити наступні: недостовірність даних, отриманих за допомогою датчиків IoT, так як окрім правильних даних, система також може збирати додаткові шуми, які не очікуються; управління гетерогенними масивними даними IoT в реальному часі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Росляков А. В. ИНТЕРНЕТ ВЕЩЕЙ : Учебное пособие / А. В. Росляков, С. В. Ваняшин, А. Ю. Гребешков. - Самара : ПГУТИ, 2015.
2. Гайкович, Г.Ф. Стандартизация в области промышленных сетей. Развитие беспроводных стандартов для АСУ ТП [текст] / Г.Ф. Гайкович //Электронные компоненты. – 2009. – №1.
3. Аналитический обзор протоколов Интернета вещей // электрон. текст. дані URL: <http://lib.tssonline.ru/articles2/reviews/analiticheskiy-obzor>
4. Протокол MQTT. Особенности, варианты применения, основные процедуры MQTT Protocol. // электрон. текст. дані URL: <http://www.mka.ru/categories/81/10416/>.
5. Протоколы «Интернета вещей»: основные сведения // электрон. текст. дані URL: <http://old.rtsoft.ru/press/articles/detail.php?ID=2718>.
6. T. Fan and Y. Chen, "A scheme of data management in the Internet of Things," in Proceedings of 2nd IEEE International Conference on Network Infrastructure and Digital Content, 2010.
7. Y. Huang and G. Li, "A Semantic Analysis for Internet of Things," in International Conference on Intelligent Computation Technology and Automation (ICICTA), May 2010.
8. M. Wu, T. Lu, F. Ling, J. Sun, and H. Du, "Research on the Architecture of Internet of Things," in 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Aug. 2010.
9. Liu Shunca. Discussion on the development of the Internet of things technology and its application of network security technology and application, 2016.
10. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660.

11. Черняк Л. Платформа Интернета-вещей // Открытые системы. СУБД. – 2012.- №7.
12. Вишневский, В. Mesh-сети стандарта IEEE 802.11s – технологии и реализация / В. Вишневский, Д. Лаконцев, А. Сафонов, С. Шпилев // Первая миля. – 2008. – №2-3.
13. R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet of Things architecture, possible applications and key challenges," in Proc. 10th Int. Conf. FIT, 2012.
14. I. Strategy and P. Unit, "ITU internet reports 2005: The internet of things," Geneva: International Telecommunication Union (ITU), 2005.
15. N. A. Ali and M. Abu-Elkheir, "Data management for the Internet of Things: Green directions," in Proceedings of the 2012 IEEE Globecom Workshops, 2012.
16. Wi-Fi HaLow (IEEE 802.11ah) — дальнобойное беспроводное подключение с низким энергопотреблением для интернета вещей // электрон. текст. дані URL: <https://www.ixbt.com/news/2016/01/05/wi-fi-halow-ieee-802-11ah.html>
17. The Basics of Bluetooth Low Energy (BLE) // электрон. текст. дані URL: <https://www.novelbits.io/basics-bluetooth-low-energy/>
18. Z-Wave // электрон. текст. дані URL: <https://ru.wikipedia.org/wiki/Z-Wave>
19. The advantages and disadvantages of Internet Of Things // электрон. текст. дані URL: <https://e27.co/advantages-disadvantages-internet-things-20160615/>
20. A Survey on Sensor-based Threats to Internet-of-Things (IoT) Devices and Applications // электрон. текст. дані URL: <https://arxiv.org/pdf/1802.02041.pdf>

21. A Survey on Sensor-based Threats to Internet-of-Things (IoT) Devices and Applications // електрон. текст. дані URL: <https://arxiv.org/pdf/1802.02041.pdf>